UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingenieros de Sistemas

TEMA:
DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS (NIDS) PARA UNA RED SIMULADA PYMES EN GNS3, IMPLEMENTADA EN UN MÓDULO RASPBERRY PI PORTÁTIL

AUTORES:
CARATE PILATUÑA BRYAN RICARDO
POZO MENDOZA DIEGO FRANCISCO

TUTOR:
JAYA DUCHE MANUEL RAFAEL

Quito, julio de 2019

CESIÓN DE DERECHOS DE AUTORES

Nosotros, Carate Pilatuña Bryan Ricardo, con documento de identificación N° 1712597317, y Pozo Mendoza Diego Francisco, con documento de identificación N° 1720024544, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación con el tema: "**DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS (NIDS) PARA UNA RED SIMULADA PYMES EN GNS3, IMPLEMENTADA EN UN MÓDULO RASPBERRY PI PORTÁTIL**", mismo que ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

Nombre: Carate Pilatuña Bryan Ricardo
Cédula: 1712597317
Fecha: julio de 2019

.....

Nombre: Pozo Mendoza Diego Francisco
Cédula: 1720024544
Fecha: julio de 2019

DECLARATORIA DE COAUTORIA DEL TUTOR

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el proyecto de titulación, "**DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS (NIDS) PARA UNA RED SIMULADA PYMES EN GNS3, IMPLEMENTADA EN UN MÓDULO RASPBERRY PI PORTÁTIL**", realizado por **Carate Pilatuña Bryan Ricardo** con ID: **1712597317** y **Pozo Mendoza Diego Francisco** con ID: **1720024544**, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, julio de 2019

Jaya Duche Manuel Rafael
Docente UPS
CI: 1710631035

AGRADECIMIENTOS

Agradecemos a la Universidad Politécnica Salesiana por haber contribuido con nuestra formación académica y personal, a nuestro tutor de titulación Rafael Jaya, que nos ha guiado durante el proceso de realización de este trabajo y más que a nadie a nuestros padres que nos han empujado y motivado en todo este camino.

Bryan Ricardo Carate Pilatuña

Diego Francisco Pozo Mendoza

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

En el mercado Ecuatoriano, las soluciones a nivel de red tienen costos altos, que no se ajustan al presupuesto de una PYME, el presente trabajo tiene por objetivo principal, implementar un sistema de detección de intrusos (NIDS) de bajo costo, usando un módulo Raspberry Pi 3 B, el sistema operativo que se utilizará es, Raspbian Stretch y el sistema de detección de intrusos, Snort. Este se evaluará en un ambiente PYME simulado en GNS3, mediante la metodología experimental, para valorar la detección de incidencias, se realizaron pruebas de intrusión controladas como: DoS y probing. Adicional a esto, se realizó una evaluación del rendimiento del módulo Raspberry Pi durante las pruebas de intrusión.

Las alertas emitidas del IDS se guardaron en logs, registrando la hora en la que ocurrió la incidencia, el tipo de incidencia, además del origen y destino del ataque. El IDS a través de diez pruebas ha demostrado que tiene una efectividad de paquetes analizados del 96,87% y un promedio de 3,13% de paquetes no resueltos, la eficiencia promedio del CPU del módulo Raspberry Pi al momento de realizar los ataques es del 1.96% del uso global del CPU desde que inicializan los ataques.

Con estos resultados se demostró que, con un bajo presupuesto, se puede desarrollar un NIDS para un escenario como el de una PYME y así beneficiarse de una mejor seguridad, alertando posibles incidencias en la disponibilidad de la red.

Abstract

In the Ecuadorian market, network solutions have high costs, which do not fit the budget of an SME, the main objective of this work is to implement an intrusion detection system (NIDS), using a Raspberry Pi 3 B module, the operating system to be used is Raspbian Stretch and the intrusion detection system, Snort. This will be evaluated in a simulated SME environment in GNS3, to assess the detection of incidents, controlled intrusion tests such as: DoS and probing will be carried out. In addition to this, an evaluation of the performance of the Raspberry Pi module will be carried out during the intrusion tests.

The alerts that are issued from the IDS will be saved in files, recording the time in which the incident occurred, the type of incident, in addition to the origin and destination of the attack. The IDS through ten tests has shown that it has an analyzed packet effectiveness of 96.87% and an average of 3.13% of unresolved packets, the average CPU efficiency of the Raspberry Pi module at the time of the attacks is 1.96% of the overall CPU usage since the attacks are initialized.

In which it was demonstrated that, with a low budget, a NIDS can be developed for a scenario like that of an SME and thus benefit from better security, alerting possible incidents in the availability of the network.

INTRODUCCIÓN

ANTECEDENTES

En el mercado nacional, las soluciones a nivel de red tienen costos altos, que no se ajustan al presupuesto de una PYME, una empresa pequeña “es considerada cuando esta tiene de 1 a 15 empleados y su volumen de negocio o balance es inferior a los $300.000.” (Valencia., 2019) Por ejemplo, el caso de una empresa pequeña de contabilidad, adquirir una solución empresarial que vigile un servidor donde se alojen las facturas puede oscilar desde los $120 por nodo hasta los $140 mil por toda la red de datos, una inversión elevada para ser implementada en una empresa de estas características, por lo que se opta por una solución de bajo costo que cumpla con la vigilancia de la red de datos en caso de intrusiones y que a la vez pueda monitorizar un nodo en especial. Un sistema de detección de intrusos cumple con estos requerimientos, por lo que esta es la solución que se propone, la metodología a utilizarse es la experimental, ya que se crea un escenario simulando una red de datos PYME, en la cual se realizan pruebas de intrusión lo que permitirá recoger datos en el NIDS, los métodos de detección de intrusos que se utilizan son dos: detección basado en firma, el cual monitorea paquetes y los compara con patrones establecidos y detección basado en anomalías, el cual monitorea tráfico y lo compara con una base establecida, posteriormente se analizaran dichos datos para demostrar que con un bajo presupuesto se puede implementar una solución NIDS aun ambiente PYME.

Los ataques que se detectarán con la solución son: denegación de servicios (DoS), ya que afecta directamente al usuario evitando la conexión a un servidor y Probing, donde se realiza un escaneo de puertos abiertos, el cual revela posibles brechas de seguridad en un servidor, estos son problemas principales para red de datos PYME.

PROBLEMA

Actualmente en el mercado nacional, las soluciones a nivel de red tienen costos altos, que no se ajustan al presupuesto de una PYME, por ejemplo el caso de una empresa pequeña de contabilidad, con un servidor de archivos y tres computadoras, adquirir una solución empresarial pueden oscilar desde los $120 por nodo hasta los $140 mil, una inversión elevada para ser implementadas en pequeñas o medianas empresas, por lo cual, no se aplica a nivel físico, en el mejor de los casos la solución queda implementada a nivel lógico o no queda implementada ninguna solución. Según el informe anual de seguridad de Cisco, las PYME son menos probables que "tengan equipos de inteligencia de amenazas y de respuesta ante incidentes que empresas más grandes." (CISCO, s.f.) , esto se debe a que estas empresas deben limitarse a un presupuesto, este problema es uno de los obstáculos más grandes que las PYME deben superar para acoger técnicas y tecnología de seguridad modernos. De acuerdo a lo expuesto, es evidente la necesidad de que las PYME también implementen algún sistema de seguridad de red avanzado, ya que a ellas "se les confía datos de los clientes" (CISCO, s.f.) , y es responsabilidad de estos "proteger esta información contra ataques online" (CISCO, s.f.) , por lo tanto hay que realizar una serie de preguntas como, ¿Cuáles han sido los diferentes tipos de ataques que sufren las PYME? ¿Hay alguna solución económica para cubrir estas brechas de seguridad informática?, para estas inquietud se deben buscar mecanismos para la detección de intrusos o ataques, de esta manera evitando que se comprometa la seguridad de la información de la empresa y de sus clientes.

JUSTIFICACIÓN

Ya que cualquier red de datos es susceptible a cualquier intento de intrusión o ataque informático, es crítico que se cuente con un sistema que permita detectar actividades sospechosas, emita alertas y que a la vez proporcione un registro de incidencias en tiempo real. Por lo general, adquirir una solución empresarial puede oscilar desde los $120 por nodo hasta los $140 mil, una inversión elevada para ser implementadas en pequeñas o medianas empresas.

Adquirir dispositivos dedicados de seguridad red, como es el IDS o un Firewall, dentro del mercado ecuatoriano llega a tener un costo alto parar el presupuesto de un PYME. La solución que se propone es mediante un módulo Raspberry Pi 3 B crear un NIDS, instalando en un sistema operativo independiente, que sea, liviano y que cumpla con los requerimientos mínimos para aplicarlo en el módulo Raspberry Pi. De esta manera, a través de software libre y una muy baja inversión, en el módulo Raspberry Pi, se podrá disponer de una seguridad de red económica y personalizable para cualquier PYME.

OBJETIVOS DEL PROYECTO

Objetivo General

Diseñar un sistema de detección de intrusos (NIDS) para una red simulada en GNS3, implementada en un módulo Raspberry Pi.

Objetivos Específicos

Diseñar e implementar un (IDS/firewall) en Raspberry Pi para soluciones de bajo costo en el área de seguridad informática.

Investigar diferentes tipos de ataques internos a la red que sufren los PYME.

Realizar pruebas de efectividad ante ataques a una red media-pequeña antes y después de la implementación, con el fin de recoger datos que permitan realizar un análisis comparativo de los mismos.

Ejecutar un análisis de tipo técnico, económico y legal.

METODOLOGÍA

Para realizar el presente proyecto se utilizará un módulo Raspberry Pi 3 modelo b, en el cual se agregó un módulo de ventilación y una tarjeta SD de 32 GB, la misma que contiene el sistema NOOBS con el cual se instalará el sistema operativo Raspbian. En la configuración de Raspbian se instalará Snort el cual es un sistema IDS, dentro de Snort, se configurará las reglas con las cuales se podrá identificar los diferentes tipos de ataques que van hacer simulados en la topología en GNS3. En la computadora física que se utilizará para la simulación, está instalado GNS3 como software de simulación y VMware como software de virtualización, dentro del gestor de máquinas virtuales se tiene virtualizado CentOS 7 con el software NMAP y Windows 7 con Apache como servidor web dentro de la topología.

Dentro de la topología en GNS3, se ha configurado un Router c3600 y un Switch, también se añadió dos nubes, una nube permite la conexión con la tarjeta de red de la computadora y la otra nube la conexión con el Raspberry Pi, se configuró dos VPCS y también se enlazó las máquinas virtuales de VMware a la topología de GNS3. Para poder conectar la computadora con el Raspberry se utilizó un adaptador de red/USB, ya que el puerto de red que viene en la computadora es utilizado para la conexión a internet, una vez realizada esta instalación y configuración tanto de forma física como de virtual, se procede con la evaluación de efectividad del IDS configurado dentro de la topología PYME simulada. Las pruebas que se realizaran son ataques distribuidos, ataques secuenciales, una prueba con el sistema IDS ejecutándose por un tiempo prolongado y se evaluara el rendimiento de los recursos del Raspberry antes y durante los ataques.

CAPÍTULO 1

Marco Teórico

En este capítulo se desarrollan conceptos y definiciones de varios autores, con el fin de tener un mejor entendimiento al momento de leer este trabajo, estas definiciones y conceptos son abarcados en el tema central del proyecto y desarrollados en el producto final.

1.1 Sistema de Detección de Intrusos (IDS)

“Ya sean amenazas o incidencias de infiltrado en una red, en general, los IDS de tipo de red preparan máquinas dedicadas para monitorear las comunicaciones que fluyen en la red en busca de comportamiento anómalo. La ubicación varía según el lugar que desee supervisar. Cuando se revela una amenaza, el IDS envía alertas a los administradores, quienes pueden tomar alguna acción.” (hispananetwork, 2018)

1.1.1 Network Intrusion Detection System (N-IDS)

“Los IDS pueden clasificarse según su ubicación en la red para detectar anomalías. De acuerdo con los objetivos a ser monitorizados por el IDS, se pueden dividir en "tipo de red (NIDS)" y "tipo de host (HIDS)". El NIDS es un sistema que intenta detectar patrones o acciones maliciosas, analizando el tráfico en la red en los paquetes entrantes como: ataques de denegación de servicio, escaneos de puertos en una red de datos o en una computadora en sí.” (GOMEZ, 2003)

1.1.2 Modo Promiscuo

“En términos de red, cuando la tarjeta de red de un computador se encuentra configurada en "modo promiscuo", esta recibe todos los paquetes del mismo

segmento de red. Una tarjeta de red, solo admite paquetes encaminados a su dirección MAC, en el "modo normal". Cuando la tarjeta de red está en "modo promiscuo", no solo admite todos los paquetes en el mismo segmento de red, sino que también los envía al OS. Este proceso es útil para capturar contraseñas, monitorizar redes y encontrar paquetes maliciosos.” (hispananetwork, 2018)

1.2 **Simulación Gráfica de Redes (GNS3)**

“El simulador de red GNS3 es un software gratuito de código abierto el cual permite diseñar topologías de red complejas, ejecutar y evaluar estas simulaciones. GNS3 funciona utilizando imágenes reales de Cisco IOS que se emulan utilizando un programa llamado Dynamips. GNS3 es realmente como la parte grafica del producto en general. Los usuarios consiguen una interfaz que les permite levantar laboratorios complejos que consisten en una variedad de enrutadores Cisco compatibles con esta GUI.” (Neuman, 2015)

1.2.1 **Arquitectura**

“El simulador GNS3 consta de dos componentes de software: la interfaz gráfica de usuario todo en uno y el servidor local o máquina virtual de GNS3.” (Telectrónika, 2018)

1.2.1.1 Programa GNS3 todo en uno

“La parte de software necesaria para la ejecución de GNS3 y la GUI del GNS3 son componentes del programa todo en uno. Este paquete todo en uno instala el software en la computadora local ya sea Linux, Windows o MAC; con lo cual se puede crear topologías de red complejas.” (Telectrónika, 2018) . A continuación en la figura 1, se puede apreciar la interfaz gráfica del usuario.

Interfaz Gráfica GNS3

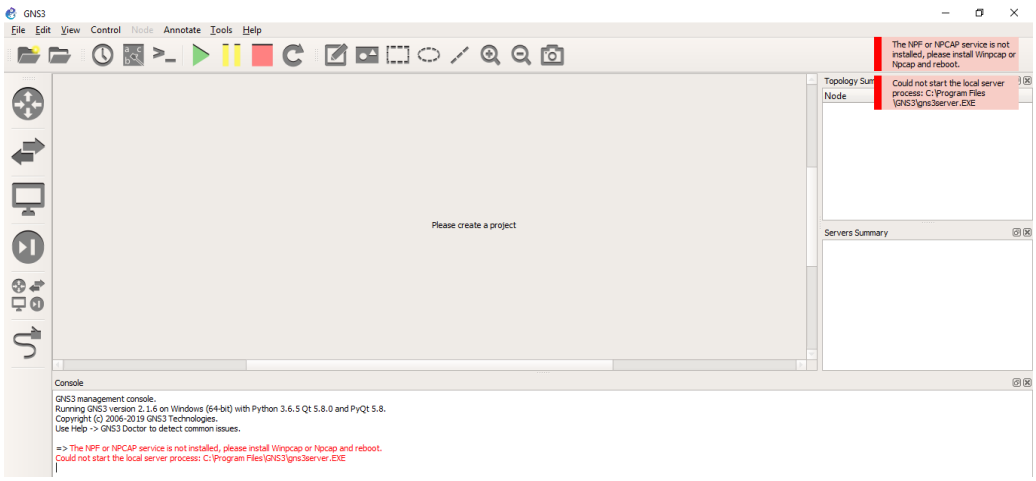

Figura 1. Interfaz gráfica de GNS3
Fuente: (Telectrónika, 2018)

Con GNS3 los usuarios tendrán la opción de escoger cada uno de los elementos que llegaran a formar parte de una red de datos.” (Universidad Complutense Madrid, 2019) GNS3 primitivamente, “solo emulaba dispositivos Cisco a través de un software llamado Dynamips, ahora GNS3 admite dispositivos de múltiples proveedores de red, incluidos Switch virtuales Cisco, Cisco ASA, BrocadevRouter, RoutersCumulus Linux y muchos otros.” (Telectrónika, 2018)

1.2.2 **Características**

Las características principales que se pueden destacar del simulador GNS3 son las que se muestran en la Tabla 1.

Tabla 1. Características de GNS3

Características de GNS3
Funciona en cualquier plataforma de sistema operativo.
Permite el diseño de redes complejas.
Permite simular una conexión de red real hacia Internet.
Permite emular varias plataformas: Cisco IOS, IPS, Firewalls ASA y PIX, Junos.
Tiene embebido los módulos: Dynamips, Dynagen, Qemu.
Permite capturar paquetes mediante Wireshark.

Fuente: (Telectrónika, 2018)

1.3 **OPNET (Optimized Network Engineering Tool)**

OPNET, "proporciona un entorno virtual de red que simula el comportamiento de una red de datos por completo, incluyendo sus pasarelas por Routers, Switches, protocolos, servidores y aplicaciones en red. Permite validar cambios en la red antes de ser implementados, diagnostica problemas de una forma eficiente y prevé el comportamiento de la red de datos ante futuros escenarios como crecimiento de tráfico." (Valonso, 2018)

La principal diferencia de OPNET en comparación con otros simuladores se encuentra en su potencia y versatilidad. "Proporciona modelos pre-construidos de protocolos y dispositivos, permite crear y simular diferentes topologías de red, el conjunto de protocolos es fijo y no se puede crear nuevos protocolos ni modificar el comportamiento de los existentes." (OPNET Projets Team. Customized OPNET Simulator Projects, 2019) .

A continuación, en la siguiente figura 2, se puede apreciar la interfaz gráfica del usuario de OPNET.

Interfaz Gráfica de OPNET

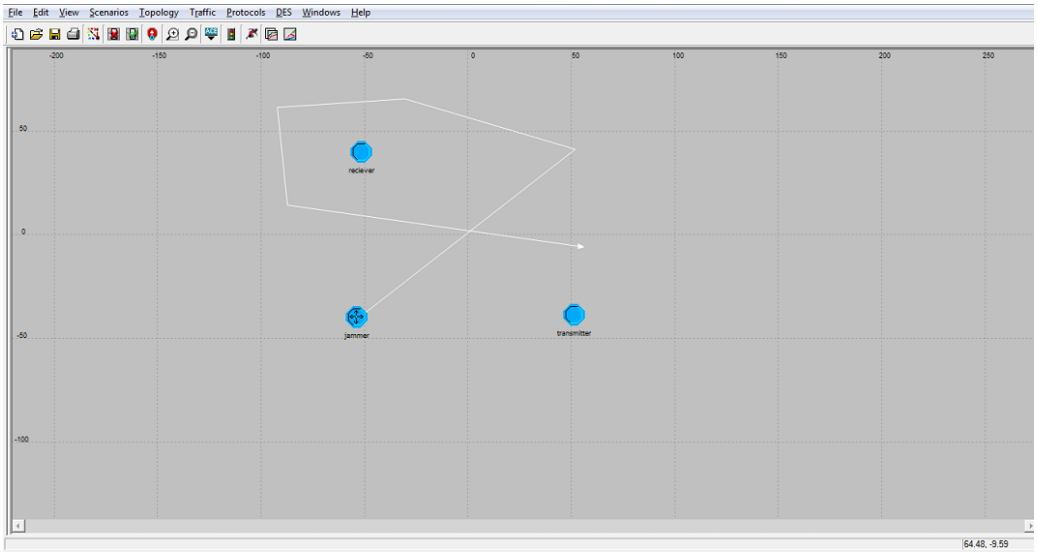

Figura 2. Interfaz gráfica de OPNET
Fuente: (OPNET Projets Team. Customized OPNET Simulator Projects, 2019) .

1.3.1 **Características**

Las características principales que se pueden destacar de OPNET son las que se indica en la tabla 2.

Tabla 2. Características de OPNET

Características OPNET
Modelo de paquetes por eventos discretos.
Modelo analítico de colas de paquetes para el tráfico que está en la forma de "flujo" de datos.
Descargable del sitio web oficial de OPNET sin costo.
Compatible con Windows 2000 y superiores.

La herramienta ACE (Application Characterization Environment) provee capacidades de visualización y diagnostico que ayudan al análisis de aplicaciones en red.
Se puede construir topologías de hasta 20 nodos (con 2 o más conexiones cada uno)

Fuente: (OPNET Projets Team. Customized OPNET Simulator Projects, 2019) .

1.4 **NMAP**

"NMAP (Network Mapper) es un programa de código libre, el cual brinda ayuda en el descubrimiento de redes y análisis de seguridad en la red. Tiene utilidad en trabajos como la supervisión del tiempo de actividad de algún dispositivo o de un servidor y el inventario de redes. NMAP para determinar que dispositivos están disponibles en la red, maneja paquetes IP sin resolver. Por ejemplo, que versión de SO se está ejecutando, que tipo de firewall está en uso o que servicios ofrece un host en específico. Otra de las utilidades de NMAP es, facilitar tareas como escanear rápidamente redes grandes, o ya sea un host en específico. NMAP tiene una opción que le permite omitir los sistemas de detección de intrusos. Por lo tanto, también se puede usar para piratas informáticos malintencionados para investigar el host objetivo de un ataque." (Lyon, 2016)

1.5 **Raspberry PI**

"Es un módulo computacional de bajo costo, una micro computadora, del tamaño relativo a una tarjeta de crédito, desarrollado por la Fundación Raspberry PI. Es un pequeño dispositivo que facilita a usuarios explorar la informática y aprender a programar en lenguajes como Scratch o Python. Es capaz de hacer todo lo que se

espera que haga una computadora de escritorio de un usuario regular.” (HALFACREE, 2012)

Por este motivo,“es una de las tarjetas más usadas por desarrolladores de sistemas embebidos, destacando su capacidad de conexión con periféricos que normalmente se encontrarían en un microcontrolador.” (E-Marmolejo, 2018)

1.5.1 **Placa de Computación (SBC)**

“Una computadora de placa única (SBC), es una computadora completa que está construida en una placa individual y contiene componentes de computadores incluyendo: el microprocesador, memoria e interfaces de entrada y salida (I/O). Las computadoras SBC suelen proveer un medio de procesamiento de datos de bajo consumo, sin ventilador y circuitos de tamaño reducido.” (LIBRE, 2014)

1.5.2 **Raspberry Pi 2**

“Presenta un procesador Cortex-A7 de cuatro núcleos en 900 MHz, tiene una memoria RAM de 1 GB, la cual es compartida con el GPU para las aplicaciones con requisitos de memoria o calculo. El núcleo del sistema operativo esta actualizado para aprovechar la tecnología ARM Cortex-A7. Tiene compatibilidad con versiones anteriores de hardware y software con la Raspberry PI 1.” (BricoGekk, 2016)

1.5.3 **Raspberry Pi 3 Modelo b**

La placa base presenta características como, “unas dimensiones de 85 x 54 milímetros, está equipado con un chip Broadcom BCM2837, Cortex-A53 (ARMv8) 64-bit, que alcanza una velocidad de hasta 1.4 MHz, su GPU es VideoCore IV de 400 MHz, cuenta con conexión Bluethooth y WIFI, su memoria RAM aumenta hasta 1GB, posee puerto HDMI y entrada Ethernet, con su nueva tecnología se puede

conectar a redes Wi-fi de banda ancha , este modelo soporta bandas desde 2.5 GHz hasta 5 GHz.” (GENERACIONYOUNG, 2018)

1.6 **Raspbian**

“Es un sistema operativo gratuito basado en Debian optimizado para el hardware Raspberry Pi. Cabe destacar que, Raspbian no está afiliado a la Fundación Raspberry Pi. Raspbian es un OS creado en comunidad por un equipo de desarrolladores que son entusiastas del hardware Raspberry Pi, los ideales educativos de la Fundación Raspberry Pi y el proyecto Debian; fue pensado para una fácil instalación en el Raspberry pi, sin embargo, Raspbian todavía está en desarrollo activo con un énfasis en mejorar la estabilidad y rendimiento.” (Thompson, 2012)

1.6.1 **Características**

En la Tabla 3, se indica las características principales de Raspbian.

Tabla 3. Características de Raspbian

Software	**Raspbian**
Modelo de Desarrollo	Software libre y código abierto
Última versión estable	8 de Abril del 2019
Núcleo	Linux
Interfaz grafica	LXDE
Plataformas Admitidas	ARM, x86, x64
Licencia	GPL

Elaborado por: Bryan Carate y Francisco Pozo

1.7 **Arch Linux ARM**

Es una distribución de Linux para computadoras ARM. “Arch Linux ARM lleva adelante la filosofía de simplicidad y centrado en el usuario, enfocado y acomodando a usuarios de Linux al darles un control completo y responsable sobre el sistema. Se

proporciona instrucciones para ayudar a navegar las modalidades de la instalación en las distintas plataformas, sin embargo, el sistema en si ofrece poca asistencia al usuario. La distribución completa se encuentra en un ciclo de lanzamiento continuo que se puede actualizar diariamente a través de paquetes pequeños en lugar de grandes actualizaciones en un calendario de lanzamiento definido.” (Arch Linux ARM, 2019)

1.7.1 **Características**

Las características principales que se pueden destacar de Arch Linux ARM son las que se indica en la Tabla 4.

Tabla 4. Características de Arch Linux ARM

Software	**Arch Linux ARM**
Modelo de Desarrollo	Software libre y código abierto
Última versión	Actualización constante
Núcleo	Linux
Interfaz grafica	LXDE
Plataformas Admitidas	ARM , x86-64
Licencia	GPL

Fuente: (Arch Linux ARM, 2019)

1.8 **Snort**

“Snort es una herramienta que se clasifica como IDS para la red. Monitoriza la salida de comunicaciones que fluyen en la red para detectar si está siendo atacado. Snort puede detectar escaneo de puertos, intento de ataques y registrar estos eventos, a la vez de emitir alertas de la incidencia. Además, al detectar comunicaciones sospechosas, se espera que evite daños, todo esto en tiempo real. Snort está bajo la licencia GNU GLP, gratuito y funciona bajo plataformas Windows y UNIX/Linux. La comunidad de Snort brinda actualizaciones de patrones prefijados ante

incidencias sobre vulnerabilidades o ataques. La colocación de Snort en la red puede realizarse según el tráfico que quieren vigilar como: paquetes que entran o paquetes salientes.” (EcuRed, 2018)

1.8.1 **Arquitectura de Snort**

Los elementos que componen el esquema básico de su arquitectura son:

Módulo de captura del tráfico: **“**captura los paquetes de la red de datos haciendo uso de la librería libpcap.” (Gómez J. L., 2009)

Decodificador**: “**forma estructuras de datos eidentifica los protocolos de enlace con los paquetes capturadosde lared. Recopila paquetes de cada uno de los clientes conectados a la red, los decodifica y se guardan en memoria, una vez que estos paquetes son decodificados son tratados mediante preprocesadores y luego son enviados al motor de detección.” (Gómez J. L., 2009)

Preprocesadores: “prepara los datos capturados para la detección o análisis. Existen diferentes tipos de preprocesadores dependiendo del tráfico capturado que se analizará.” (Gómez J. L., 2009)

Motor de detección: “analiza los paquetes capturados para detectar ataques, consiste en comparar los paquetes leídos con las reglas definidas, estás son agrupadas por categorías, cuando el paquete coincide con alguna de las reglas se pasa a la siguiente capa.” (Gómez J. L., 2009)

Archivo de reglas: “definen un conjunto de reglas que se seguirán en el análisis de los paquetes detectados, ya sean reglas predefinidas o personalizadas.” (Gómez J. L., 2009)

Plugins de detección: “partes del software que son compilados con el sistemaSnort y se usan para modificar el motor de detección.” (Gómez J. L., 2009)

Plugins de salida**:** “permiten definir qué, cómo y dónde se guardan las alertas de los correspondientes paquetes de red que se capturaron. Pueden ser archivos de texto, bases de datos, servidor syslog, etc.” (Gómez J. L., 2009)

1.9 **Soluciones IDS Licenciadas**

A continuación, se presentará dos soluciones licenciadas en el mercado, se describirá cuál es su funcionalidad, previo a la descripción de la factibilidad económica.

1.9.1 **QRadar Network Insights 1901**

Es un dispositivo IBM, “el cual proporciona un análisis detallado de los flujos de red para ampliar las capacidades de detección de amenazas. El rendimiento de este dispositivo varía según la configuración y el ajuste de los componentes del sistema, está influenciado no solo por el hardware, sino también por factores como los criterios de extracción y la cantidad de datos de la red.” (IBM, 2014)

Tabla 5. Características de QRadar Network Insights 1901

Hardware	**Descripción**
Dimensiones	28.9 pulgadas de profundidad x 17.1 pulgadas de ancho x 1.7 pulgadas de alto
Poder	Fuente de alimentación CA doble redundante de 750 vatios
Almacenamiento	2 x 240 GB SATA 2.5 "SSD, 240 GB en total (RAID1)
Memoria	64 GB (4 x 16 GB DDR4 2400MHz)
Transceptores de captura de red	2 x 1 G TX RJ-45 Transceptores (Avago ABCU-5710RZ o ABCU-5740RZ)

	2 x 1 G SX LC Transceptores (Avago AFBR-5715PZ)
Transceptores de gestión de red.	SFP de corto alcance 2 x 10 G
	Los transceptores pueden tener uno de los siguientes números de pieza:
	Avago AFBR-709SMZ-IB8
	Finisar FTLX8571D3BCL-BN
	BNT BN-CKM-SP-SR

Fuente: (IBM, 2014)

1.9.2 **Symantec Critical System Protection**

"Symantec Critical System Protection 5.2.6 protege el tiempo de inactividad físico y virtual del servidor, con la prevención y detección de vulnerabilidades conocidas y desconocidas que afectan a los sistemas. Aproveche el comportamiento del sistema de seguridad y el firewall del host, la prevención de intrusiones y ataques. La consola de administración centralizada permite a los administradores configurar y mantener políticas de seguridad, administrar usuarios y roles, ver alertas y ejecutar informes en sistemas operativos heterogéneos." (Sysmantec Corporation, 2019)

Tabla 6. Características de Symantec Critical System Protection

	Sistema Operativo	Requisitos de Sistema
Symantec CriticalSystemProtection Management Server	· Windows 2000 Server / Windows Server 2003 / Windows Server 2008, 32-bit and64-bit · SQL Enterprise Server 2005 SP2, SQL Enterprise Server 2005 Express, SQL Enterprise Server2008, 32-bit and64-bit	· 1 GB de espacio en disco · 1 GB de RAM
Symantec CriticalSystemProtection Management Console	· Windows 2000 Server / Windows Server 2003 / Windows XP, 32-bit and64-bit · Java client o WebConsole	· 150 MB de espacio en disco · 256 MB de RAM
Microsoft Windows NT - Agent	· Windows NTServer	
SUSE Enterprise Linux (8, 9 y10)	· x86 32-bit, Intel EM64T o plataformas AMD 64	
Red Hat Enterprise Linux ES (3.0 , 4.0, 5.0 y RHEL PAE	· x86 32-bit, Intel EM64T o plataformas AMD 64	
Sun Solaris	· Sun SPARC; EM64T o plataformas AMD 64	
VMWare ESX 3.5	· x86	
IBM AIX 5L	· POWER PC	
HP-UX 11.23 y 11.31 (11i v2 y v3)	· PA-RISC o Itanium 2(IA64)	
HP-UX 11.i (11.11)	· PA-RISC	

Fuente: (Sysmantec Corporation, 2019)

1.10 **VMware**

"Es un software de virtualización que permite que múltiples sistemas operativos se ejecuten en una sola computadora. Esto significa que permite ejecutar múltiples entornos en su escritorio sin reiniciar. VMware reconoce la interoperación entre sistemas operativos, también permite aislar y proteger los entornos operativos

individuales, esto puede ser útil en la evaluación de soluciones de IT, prueba de aplicaciones o demostración de productos.” (VMware, Inc., 2019)

A continuación, en la siguiente figura 5, se presenta la interfaz gráfica de usuario de VMware.

GUI de VMware

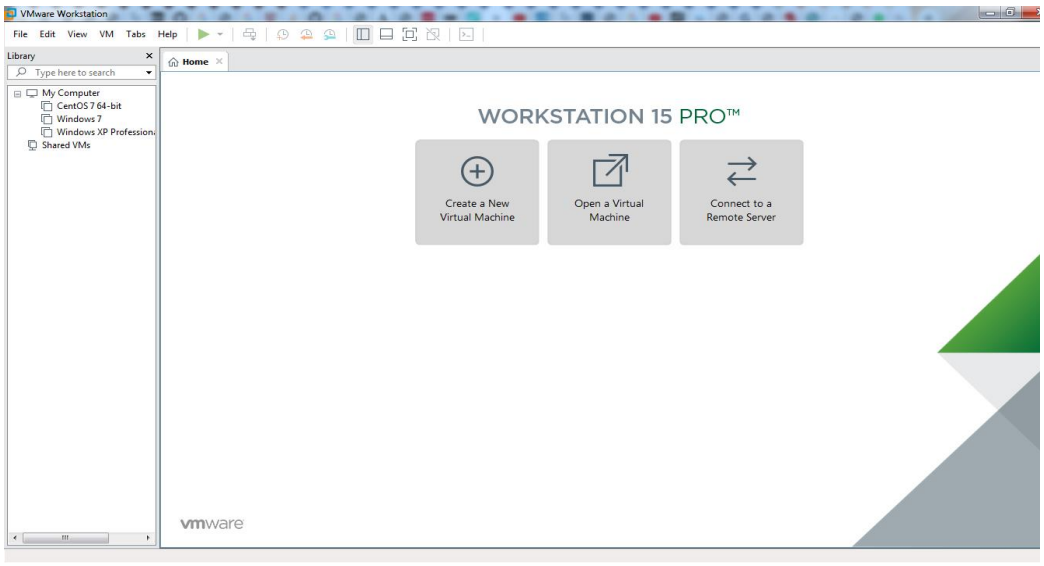

Figura 3. Interfaz gráfica de VMware.
Elaborado por: Bryan Carate y Francisco Pozo

1.10.1 **Características de VMware**

Las características principales que se pueden destacar de VMware son las que se indica en la Tabla 7.

Tabla 7. Características de VMware

Características de VMware
Herramientas y funciones para entornos empresariales.
Permite compartir archivos fácilmente entre el host y el sistema virtualizado.
Es compatible con lectores de tarjetas inteligentes.
Soporte para USB 3.0.
Permite crear instantáneas para restaurar el estado de una VM fácilmente.
Cuenta con una herramienta para compartir máquinas virtuales.
Se integra con vShepere7ESXi y vCloud Air.
Gráficos 3D compatibles con DirectX 10 y OpenGL 3.3

Fuente: (VMware, Inc., 2019)

1.11 **Virtual Box**

"Es una aplicación de virtualización multiplataforma, esto significa que, se instala en sus componentes existentes basadas en Intel o AMD, ya sea que estén ejecutándose los sistemas operativos Linux, Mac OS X, Windows u Oracle Solaris OS. Amplia las capacidades del computador existente para que pueda ejecutar múltiples sistemas operativos, dentro de múltiples máquinas virtuales, al mismo tiempo. Puede instalar y ejecutar tantas máquinas virtuales como se desee, los únicos límites prácticos son el espacio de disco y la memoria. VirtualBox es aparentemente simple pero poderoso, puede ejecutarse en todas partes, desde pequeños sistemas integrados o máquinas de clase de escritorio hasta implementaciones de centros de datos e incluso entornos de nube." (Oracle VM VirtualBox, 2019)

A continuación, en la figura 6, se puede apreciar la interfaz gráfica de usuario de VM VirtualBox.

GUI de VirtualBox

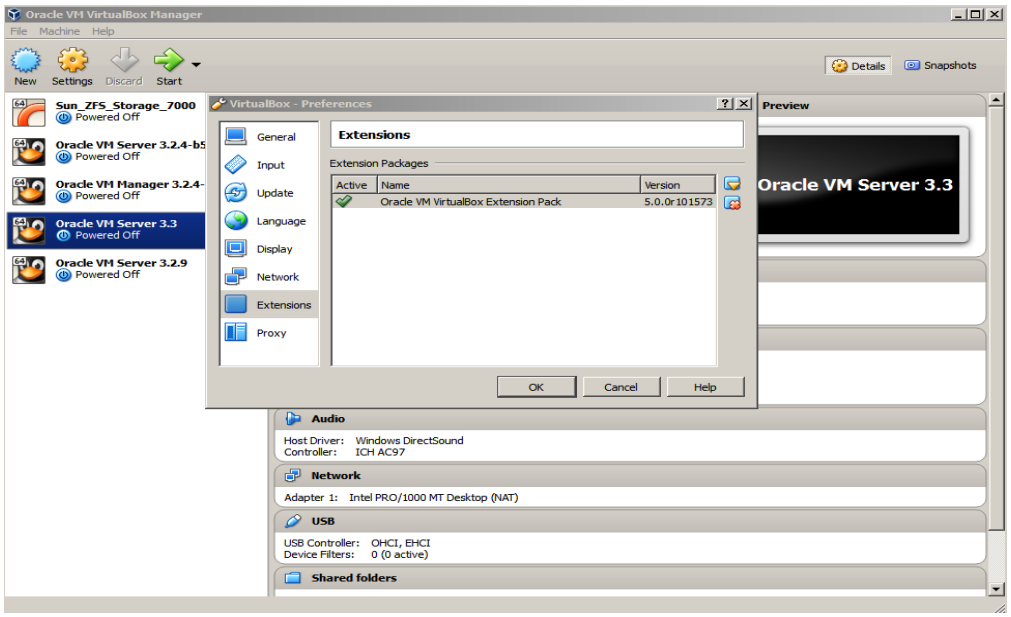

Figura 4. Interfaz gráfica de VirtualBox.
Fuente: (Virtualization, 2015)

1.11.1 **Características**

Las características principales que se pueden destacar de VM VirtualBox son las que se indica en la Tabla 8.

Tabla 8. Características de VM VirtualBox

Características de VM VirtualBox
Es una herramienta multi-plataforma compatible con Windows, Mac OS, Linux y Solaris.
Puede controlarse a través de símbolo del sistema.
Cuenta con herramientas especiales para compartir archivos entre máquinas.

Permite crear instantáneas para restaurar el estado anterior de un VM fácilmente.
Soporte limitado para gráficos 3D.
Permite utilizar aplicaciones virtualizadas como si se trataran de aplicaciones del sistema “separándolas”.
Es compatible con las máquinas virtuales de VMware.
Cuenta con una herramienta de captura de video.
Cifrado de unidades virtuales.
Soporte para puerto USB. 2.0 y 3.0

Fuente: (Oracle VM VirtualBox, 2019)

1.12 **Hardware y Software Libre**

Para entender este concepto, “se debe entender la definición de hardware libre y software libre. El hardware libre: son los dispositivos cuyas especificaciones y diagramas son de acceso público, de manera que cualquiera pueda replicarlos. El software libre: son los programas informáticos cuyo código es accesible por cualquiera para que, quien desee pueda utilizarlo y modificarlo.” (FM, Yúmbal, 2018)

1.12.1 **Características**

Las características principales que se pueden destacar de Open Source son las que se indica en la Tabla 9.

Tabla 9. Características de Open Source

Open Source	Características
Controlar	Se puede examinar el código para una posterior edición.
Formación	El código fuente es de acceso público, los usuarios pueden modificarlo.
Seguridad	Es seguro y estable a comparación del software privado, debido que es software de código abierto alguien podría detectar y corregir errores u omisiones que los autores originales de un programa podrían haber omitido.
Robusto	Su facultad de hacer frente a errores durante la ejecución y detectar una entrada errónea.

Fuente: (FM, Yúmbal, 2018)

1.12.2 **Ventajas**

- "La calidad de desarrollo de algún sistema físico o lógico mejora en cuando su código fuente se transmite, se prueba y se corrige en comunidad." (Pickett, 2019)
- "Ofrece una oportunidad de aprendizaje, puede generar nuevas habilidades a programas actualmente disponibles." (Pickett, 2019)

- “Es más seguro que el software privado, porque al identificar errores en comunidad, se solucionan rápidamente.” (Pickett, 2019)

- “Dado que está en el dominio público y está sujeto a actualizaciones, hay pocas posibilidades de que no esté disponible, lo que es un ventaja para proyectos a largo plazo.” (Pickett, 2019)

1.13 **Tipo de Ataques a las PYME**

Tomando en cuenta “el avance en la tecnología, las empresas sean públicas o privadas, toman medidas de protección y seguridad para preservar la información, ya que se han hecho presentes ataques informáticos e infiltraciones no autorizadas de personal ajeno o mal intencionado para cometer acciones ilícitas o sacar ventajas competitivas.” (Vega Villacís, 2017)

Se tiene la necesidad de saber cuáles son los ataques que sufren las PYME. En la página web de ABC en español se menciona que, “El 43% de los ataques a nivel global se concentran en las empresas pequeñas.” (Natour, 2017) En la página web Destino negocio auspiciada por Movistar México, menciona que, las amenazas más frecuentes son las siguientes:

- Scam: “Es una modalidad de estafas a través del correo electrónico o páginas web fraudulentas. Es el típico mensaje que te pide entregar datos personales a cambio de algo. También las webs que aseguran que eres el ganador de celulares de alta gama, viajes o cupones promocionales son en muchos casos un tipo de scam.” (Destino Negocio, 2016)

- Bot: “Es un programa que le permite a un ciber delincuente tomar el control de un equipo infectado. Por lo general, son parte una red de máquinas afectadas (botnets). Los equipos infectados son conocidos como “zombis” y pueden usarse para llevar a cabo un ataque masivo de denegación de servicio.” (Destino Negocio, 2016)
- Backdoor: “Como su nombre lo indica es una puerta trasera que existe en algunos sistemas que permiten el acceso remoto a la infraestructura. Muchas veces se accede a los datos sin que las protecciones de los sistemas se den cuenta, por lo general ocurre cuando existen puertos abiertos.” (Destino Negocio, 2016)
- Exploit: “Es una amenaza que ataca una vulnerabilidad del sistema o de un software determinado. Suele instalarse en equipos corporativos como en los equipos personales con el fin de acceder a información específica. En muchos casos los exploits dependen de que el usuario atacado realice una acción determinada como abrir un archivo.” (Destino Negocio, 2016)
- Gusano: “Los gusanos son amenazas capaces de copiarse a sí mismos una y otra vez incluso infectando otros dispositivos enviando copias de sí mismos. No suelen apropiarse del control de una terminal, sino que influyen tanto en su funcionamiento como en el de la red en la que se trabaja.” (Destino Negocio, 2016)

1.13.1 **Denegación de Servicio (DDOS)**

“Un ataque DDOS tiene como objetivo anular la conexión a un servidor o una infraestructura. Existen varias formas de ataques DDOS, uno es por ocupar todo el

ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico.” (OVH innovation for Freedom, 2019)

En Ecuador los ataques DDOS se han hecho comunes en las PYME, “estos ataques hacen que los sitios web sean lentos o inaccesibles, impiden que los usuarios accedan a cuentas en línea e interrumpen las actividades comerciales.” (Federal Bureau of Investigation, 2017)

En la figura 7, se muestra el funcionamiento de un ataque DDOS

Estructura de DDOS

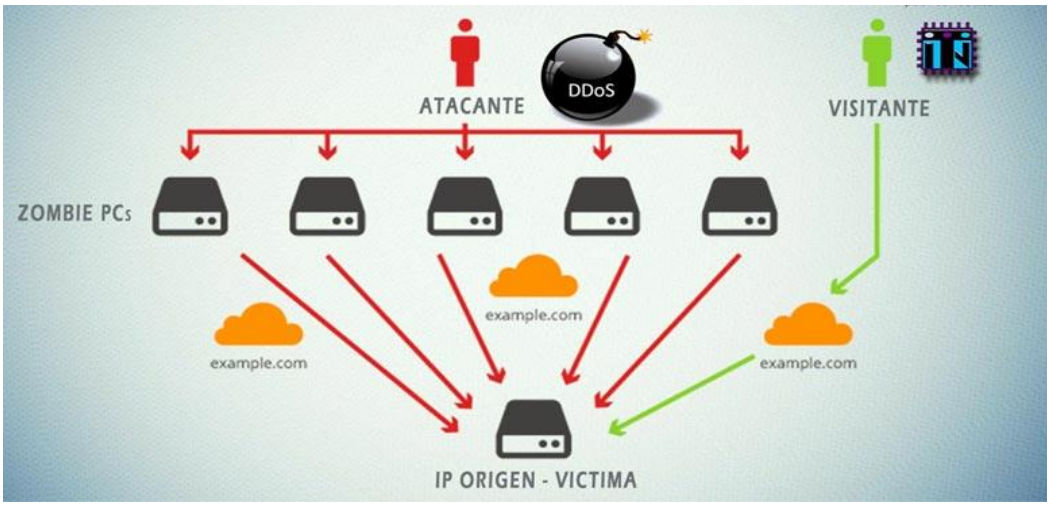

Figura 5. Estructura de ataques DDOS.
Elaborado por: Bryan Carate y Francisco Pozo

Los ataques son dirigidos de diferentes partes del mundo, en la figura 8. Se muestra en porcentaje el origen de los países de donde se hacen los ataques DDOS.

Origen de ataques DDOS

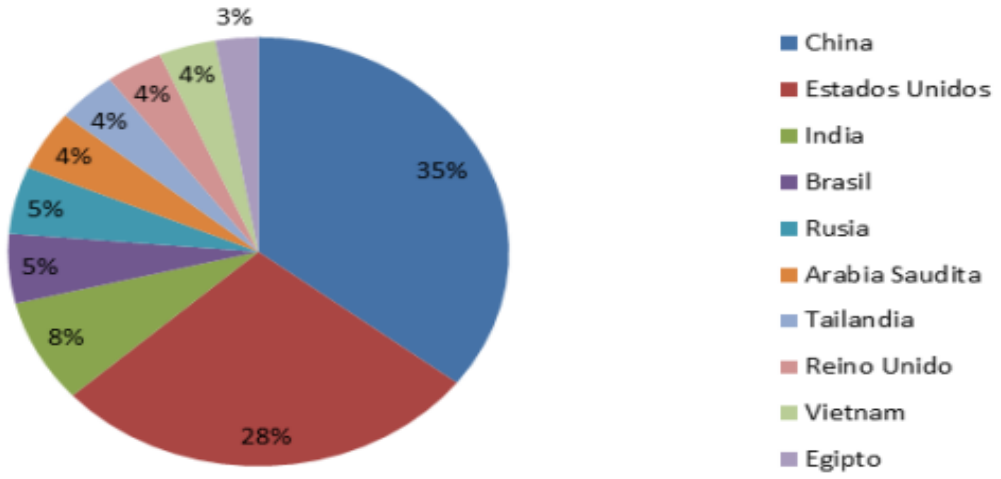

Figura 6. Porcentaje de ataques de DDOS.
Fuente: (Federal Bureau of Investigation, 2017)

1.13.2 **Probing**

"Estos ataques se denominan ataques de vigilancia y escaneo. El ataque Probing sondea las redes para encontrar clientes en la red o servicios disponibles y recopilar información sobre ellos, a partir de esta información un atacante crea una lista de vulnerabilidades que pueden usarse posteriormente para lanzar un ataque contra los hosts o entidades seleccionadas." (Alnour Ibrahim, Albdri Mohmed, Abdallah Abusham, & Mohmed Ali , 2017)Existen varios tipos de ataques de Probing como:

Barrido de IP: "escanea los clientes de la red en busca de un servicio destino en un puerto especifico." (Alnour Ibrahim, Albdri Mohmed, Abdallah Abusham, & Mohmed Ali , 2017)

Barrido de puerto: "escanea puertos para encontrar servicios disponibles en un solo cliente." (Alnour Ibrahim, Albdri Mohmed, Abdallah Abusham, & Mohmed Ali , 2017)

1.14 **Port Mirroring**

"Duplicación de puertos, Port Mirroring o SPAN (Switched Port Analyzer), es una técnica para analizar el flujo de datos en la red. Habilitando la duplicación de puertos, el Switch asigna una copia de todos los paquetes de red vistos en un puerto a otro puerto, donde se puede examinar el paquete. La función Port Mirroring es compatible con la mayoría de Switches de clase empresarial en otras palabras los Switches administrados." (MiaRec, Inc., 2019)

1.14.1 **Funcionamiento de Port Mirroring**

La duplicación de puertos es necesaria para el análisis del tráfico en un Switch porque, normalmente, un Switch envía paquetes solo al puerto al que está conectado el dispositivo de destino. En la figura 9, se pude apreciar cómo funciona un Switch normalmente.

Funcionamiento del switch

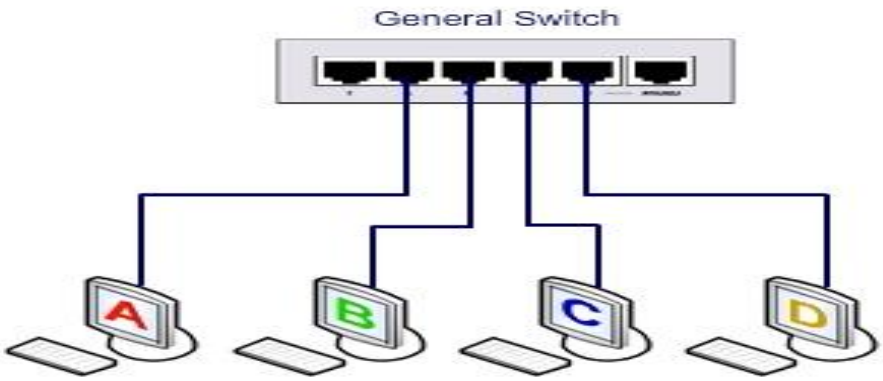

Figura 7. Funcionamiento de un switch.
Fuente: (Miarec, 2018)

Como se mencionó en la sección anterior, una vez que en el Switch se habilita la opción de Port Mirroring, se envía a un puerto destino una copia de todos los

paquetes vistos en la red, los cuales serán analizados por un sistema. Esto se puede apreciar en la siguiente figura 10.

Switch con Port Mirroring

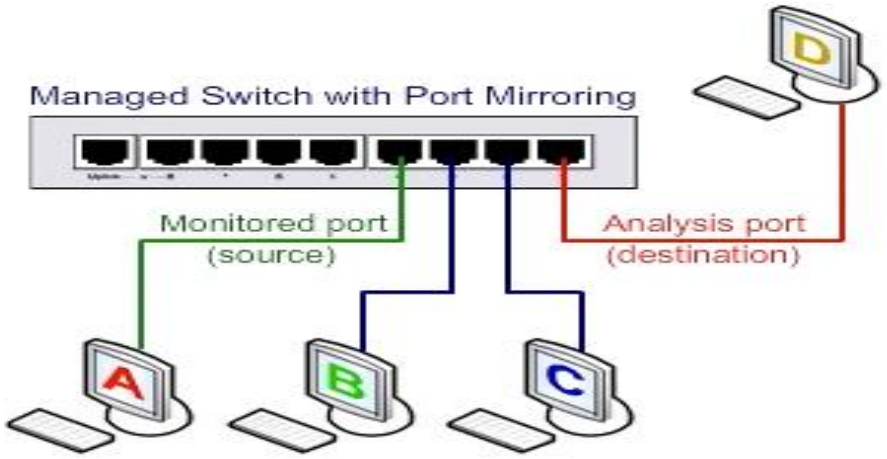

Figura 8. Funcionamiento del switch con Port Mirroring.
Fuente: (Miarec, 2018)

CAPÍTULO 2

En este capítulo se va a tratar temas como el análisis de hardware y software, donde se explica que llevo a tomar la decisión en la elección de componentes de hardware y que herramientas de software se utilizarán, se realizará un análisis técnico, económico y legal, donde se explica la factibilidad de la propuesta final.

2.1 Análisis de Hardware y Software

2.1.1 Análisis de Hardware

Para realizar el análisis de hardware se toma en cuenta cualidades como precio, compatibilidad con diferentes tecnologías entre otras características.

2.1.1.1 Raspberry PI 3 y Raspberry PI 2

A continuación, en la Tabla 10, se presenta una comparación entre las características técnicas del Raspberry Pi 2 y el Raspberry Pi 3.

Tabla 10. Comparativa de Raspberry Pi 2 y Pi 3

Características	Raspberry Pi 2 Model B	Raspberry Pi 3 Model B
Sistema de chip	Broadcom BCM2836	Broadcom BCM 2837
CPU	900 MHz Quad Core Cortex-A7 ARM11 32 bit	1.2 GHz quad core Cortex-A53 ARMv8 64 bit
GPU	Dual Core VideoCore IV® 400 MHz (3D 250 MHz)	Dual Core VideoCore IV® 400MHz (3D 300MHz)
Memoria	1GB DDR2 450MHz	1GB DDR2 450MHz
Fuente de alimentación	Conector micro USB B socket 5V 2A	Conector micro USB B socket 5V 2.5A
Consumo máximo de energía	Alrededor de 9 W	Alrededor de 12.5W
Wired LAN	10/100 Base-T RJ45	10/100 Base-T RJ45
Wireless LAN	Ninguno	IEEE 802.11 b / g / n 2.4 GHz (Broadcom BCM 43143)
Bluetooth	Ninguno	Bluetooth 4.1, Bluetooth Low Energy (Broadcom

		BCM43143)
USB	USB 2.0 x 4	USB 2.0 x 4

Fuente: (俺の技術メモ, 2016)

"Raspberry PI 3 tiene una variedad de mejoras de rendimiento y capacidades de alta velocidad, tiene funciones de conectividad inalámbrica como WI-FI, Bluetooth 4.1, Ethernet más rápido y PoE, mientras que Raspberry PI 2 carece de estas características; además del aumento en la velocidad del procesador y su cambio de 32 bits a 64bits, en términos de integración con diferentes dispositivos, se prefiere Raspberry PI 3 en lugar de Raspberry PI 2." (EDUCBA (Corporate Bridge Consultancy Pvt Ltd), 2018)

2.1.1.2 Elección Módulo Raspberry Pi

Los puntos que destacan con la versión nueva del módulo Raspberry Pi 3 son los que se indica en la Tabla 11.

Tabla 11. Características mejoradas en Raspberry Pi 3

Características mejoradas en Raspberry Pi 3
El CPU acelero de 900 MHz a 1.2 GHz.
El CPU cambio de 32 bits a 64 bits.
El rendimiento de GPU 3D aumento en 50 MHz
La tarjeta Wi-Fi fue instalada de manera estándar
El modulo Bluetooth fue instalado de manera estándar

Fuente: (EDUCBA (Corporate Bridge Consultancy Pvt Ltd), 2018)

Según los requerimientos en el libro Snort for Dummies, “se recomienda usar un procesador de 64 bits, ya que los sensores de Snort ocupan una considerable carga en el CPU.” (Scott, Wolfe, & Hayes, 2004)La preferencia de (EDUCBA (Corporate Bridge Consultancy Pvt Ltd), 2018) al preferir el Raspberry Pi 3, por su integración con otros dispositivos, es un motivo que es tomado a consideración. Por poseer un procesador de 64 bits y al ser este un requisito para implementar el IDS. El módulo Raspberry Pi 3 será el que se seleccionará para alojar el sistema operativo y el IDS.

2.1.1.3 Adaptador de Red

2.1.1.3.1 Tarjeta de Red Trendnet TU2- ET100 v3.0

“El TU2-ET100 v3.0 es una tarjeta de red USB de alta velocidad que permite conectarse a una red a 10/100 Mbps, ya sea, PC o Notebook. Además, es compatible con USB 2.0 y tienen compatibilidad regresiva a USB 1.0 o 1.1 por lo que se podrá obtener acceso a internet o una red de datos.” (TRENDnet, inc., 2019)

En la Tabla 12, se indica las características técnicas de NIC TRENDnet.

Tabla 12. Características de NIC TRENDnet

Hardware	**TU2-ET100 v3.0**
Estándares	USB 2.0, 1.1 IEEE 802.3 10Base -t
Velocidad Transferencia de datos	Ethernet: 10Mbps/20Mbps Fast Ethernet: 100Mbps/200Mbps
Compatibilidad con OS	Windows 98SE/ME/2000/XP/7, Mac OS X
Gestión de alimentación eléctrica	Modo de suspensión Modo de Hibernación

Fuente: (TRENDnet, inc., 2019)

2.1.2 **Análisis de Software**

A continuación, se realizará una comparativa entre los gestores de máquinas virtuales, simuladores gráficos de redy sistemas operativos, donde se explicará por qué se tomó de la decisión en la elección de cada software.

2.1.2.1 Elección de Gestor de Máquinas Virtuales

En esta comparativa se observa que, ambas aplicaciones son similares en cuanto a rendimiento de las máquinas virtuales, VMware utiliza memoria RAM de forma que permita acelerar las transacciones de los archivos en sus discos duros virtuales. La interfaz gráfica de VMware es amigable para los usuarios que están comenzando con la experiencia de virtualización, además a esto, la integración y compatibilidad de VMware con GNS3 es un factor que se debe tomar en consideración. En el caso de VirtualBox, se debe tener una experiencia previa o estar familiarizado con los componentes de un virtualizador.

Por lo tanto, el factor definitivo para la elección del gestor de máquinas virtuales es la integración y compatibilidad de VMware con GNS3, siendo VMware el gestor de máquinas virtuales que alojara CentOS 7 y Windows 7 Professional.

2.1.2.2 Elección de Simulador de Red

A continuación en la Tabla 13, se realiza una comparación entre GNS3 y OPNET, de esta forma definiendo cual será el simulador de red que se seleccionará.

Tabla 13. Características de GNS3 v2.1 y OPNET

General	GNS3 v2.1	OPNET
Idioma	Alemán, chino, español, italiano, portugués, coreano	Ingles
Licencia	GNU GLP v2 Open Source	Software propietario con licencia gratuita renovable cada 6 meses para entornos educativos.
Sistema Operativo	GNU/Linux Microsoft, Windows, Mac	Microsoft Windows
Descripción	Simulador grafico de red que permite la virtualización de redes, lo más cercano a los dispositivos reales, es lenta en la integración con otras aplicaciones.	Cuenta con un conjunto de protocolos y tecnologías, que permite planificar, modelar y simular redes, es un lenguaje de simulación orientado a las comunicaciones.
Requerimientos mínimos para la instalación	16 MB para Dynamips, más la cantidad que cada imagen IOS del Router real requiera y 40 MB de disco.	RAM 512 MB y HD 2 GB

Elaborado por: Bryan Carate y Francisco Pozo

GNS3 junto con Dynamips permiten personalizar las configuraciones de Switches y Routers de forma real, además de permitir una conexión simulada a Internet, en cambio OPNET está enfocado en la personalización de tráfico con un modelo analítico de colas de paquetes. Por lo tanto se elegirá GNS3 como el simulador que aloje la topología de la red PYME.

2.1.2.3 Elección de Sistema Operativo

Para evaluar los OS se realizó una ponderación que empieza desde 1 que es una calificación más baja, hasta 5 la calificación más alta, como se indica en la Tabla 14.

Tabla 14. Valoración según criterio personal

RESPUESTAS	VALOR
Excesivamente importante	10
Significativamente importante	7
Igualmente importante	5
Significativamente menos importante	2
Excesivamente menos importante	1

Elaborado por: Bryan Carate y Francisco Pozo

En la Tabla 15, se presenta una comparación de entre la valoración que se le ha asignado a los dos sistemas operativos Raspbian y Arch Linux ARM, para tomar una decisión sobre qué sistema operativo se elegirá.

Tabla 15. Arch Linux ARM y Raspbian

Software	Arch Linux ARM	Raspbian
Modelo de Desarrollo	5	5
Última Versión	7	10
Núcleo	5	5
Interfaz Gráfica	5	5
Plataformas Admitidas	5	5
Licencia	5	5
Total	32	35

Elaborado por: Bryan Carate y Francisco Pozo

Como se observa en la Tabla 15, las características de Arch Linux ARM y las de Raspbian son similares, por lo cual, las dos opciones son adecuadas, pero tomando

en cuenta que el proyecto se basa en Raspberry Pi, se utilizará la versión más actual de Raspbian. Ya que el sistema operativo Raspbian (Stretch) fue desarrollado exclusivamente para Raspberry Pi, este sistema operativo será el que alojará el sistema de detección de intrusos.

2.2 **Análisis Técnico, Económico y Legal**

En el análisis técnico y económico se realizará una comparación entre diferentes soluciones IDS en el mercado, comparando sus funciones, costos y especificaciones.

2.2.1 **Análisis Técnico y Económico**

2.2.1.1 Ubicación de IDS de Cisco en el Mercado

Snort al ser un proyecto de código libre de Cisco, se precisa saber cuál es su ubicación en el mercado frente a otras soluciones IDS, por lo cual, se hace referencia al cuadrante de Gartner.

Cuadrante de Gartner

Figura 9. Cuadrante de Gartner.
Fuente: (TRENDnet, inc., 2019)

La empresa Trend Micro realizó una petición a Gartner en el 2018 para que evalué su producto IDS frente a otras marcas, en el cual, se destaca la presencia de Cisco dentro del cuadrante de líderes en sistemas de detección y prevención de intrusos; evidenciando que, Cisco es líder en el mercado encabezando el desarrollo de IDS, lo que indica que hacer uso de Snort como sistema de detección de intrusos es una opción viable para ser implementada en un ambiente PYME.

2.2.1.2 Comparación Entre Soluciones IDS

Con los datos de Snort en la sección 1.8 y los datos de las dos soluciones IDS licenciadas en la sección 1.9, se puede elaborar un cuadro comparativo entre soluciones IDS, como se indica en la Tabla 16.

Tabla 16. Comparativa con soluciones similares

	Snort	**QRadar Network Insights**	**Symantec Critical System Protection**
Costo	Es Software Libre no tiene costo. y $120 de hardware	$134,000 por costo de licencia de instalación + Appliance.	$120.00 por nodo en la red.
Tipo de distribución	Software Libre	Software Propietario	Software Propietario
Requerimientos mínimos	4 GB libres en espacio en disco, 512 RAM, Pentium II 266 MHz	Appliance 1901 (MTM 4412-F4Y)	**Consola de administración** 150 MB libre en espacio en disco, 512 MB RAM, Pentium III 1.2 GHz **Servidor de administración** 1 GB libre en espacio en disco , 2 GB RAM, Pentium III 1.2 GHz **Agente** 100 MB libre en espacio en disco, 256 MB RAM, Pentium III 1.2 GHz
Espacio en Rack	Según el equipo en el que se instale	1 Unidad de Rack	Según el equipo en el que se instale
Requerimientos adicionales	Ninguno	Módulo de captura de paquetes (SFP), Módulo de puertos administrables (10 GbE SFP+)	Ninguno
Propietario del sistema	Cisco	IBM	Symantec

Elaborado por: Bryan Carate y Francisco Pozo

Se puede destacar que, la solución IDS que se propone no tiene costo por licencia, tiene requisitos de hardware más bajos que el de su competencia, su fabricante Cisco es líder en el cuadrante de Gartner en soluciones IDS y que la inversión aproximada de implementación es de un total de $120, como se muestra en la tabla a continuación desglosando el costo de implementación.

Tabla 17. Costo de implementación

DETALLE	COSTO
Raspberry Pi3 B	64,99
Módulo de Refrigeración	10,00
Acrílico de protección	10,00
Tarjeta SD 32 GB	15,00
Mano de obra	20,00
Total	119,99

Elaborado por: Bryan Carate y Francisco Pozo

2.2.1.3 Factibilidad Técnica y Económica

Basándose en que el presupuesto anual para invertir en tecnología para una PYME en el Ecuador, "oscila aproximadamente entre los $200 y $2000." (Tapia Cuesta, 2017) Y tomando en consideración que México, a pesar de ser una de las economías en Latinoamérica que encabezan el crecimiento regional, "en México, sólo el 33% de las Pymes invierte $126 dólares anualmente en promedio en tecnología, ya sea por necesidad o por conciencia de que es una herramienta que incrementa su productividad." (Des16)

La opción Snort como solución IDS, desde un plano financiero se puede decir que, implementándose en un módulo Raspberry Pi ante el presupuesto de una PYME es accesible, ya que $120 significa el costo de implementación de la solución, no se

tiene que cubrir el costo de hardware propietario de grandes capacidades, ni costo de licenciamiento.

Realizando un promedio del valor mínimo y del valor máximo del rango del presupuesto para una PYME se obtiene que,

$$media = \frac{valor\ minimo + valor\ maximo}{2} \qquad \text{Ec. 1}$$

Donde, el valor de la media es $1100.

El valor $120 que representan el costo de la implementación, es el 10.91% del presupuesto promedio anual de una PYME en el Ecuador.

Esto se puede calcular mediante una regla de tres simple:

$$x = \frac{\$120 * 100\%}{\$1100} \qquad \text{Ec. 2}$$

Donde, x es igual a 10.91%.

Desde un plano técnico se puede decir que, el módulo Raspberry Pi está por encima de los requerimientos mínimos para alojarla solución IDS, esta solución ayuda a detectar amenazas en tiempo real, se puede personalizar las reglas o importar una lista de reglas desde el repositorio en comunidad del IDS, evidenciando que, es factible la implementación de un módulo Raspberry Pi 3 como un IDS en una topología de red PYME, por el bajo costo de la implementación y las características que conlleva una red de estas dimensiones.

2.2.2 **Análisis Legal**

Para realizar un análisis legal, es inminente enumerar las problemáticas o amenazas legales que se tendrían por utilizar software o hardware en la solución que se

propone, a continuación, se muestran temas relevantes que se deben tomar en consideración al implementar una solución como es el de un sistema de detección de intrusos:

- Se debe adquirir licencias para evitar el uso no autorizado de software.
- Se pueden hacer cambios al hardware.
- En el caso de alguna incidencia se pueden usar los reportes como evidencia para tomar alguna acción legal.

2.2.2.1 Uso Fraudulento de Software o Hardware

Según la legislación, existen leyes las cuales penalizan el, uso fraudulento o la alteración de un sistema informático. Esto se puede verificar en el código orgánico integral penal, en los artículos: 190 (Apropiación fraudulenta por medios electrónicos) el cual indica que "La persona que utilice fraudulentamente un sistema informático alterando, manipulando o modificando el funcionamiento de sistemas informáticos será sancionada con pena privativa de libertad de uno a tres años." (Ministerio de Justicia, Derechos Humanos y Cultos, Subsecretaría de Desarrollo Normativo, 2014) , 232 (Ataque a la integridad de sistemas informáticos) el cual indica que "La persona que altere a todo o partes de sus componentes lógicos que lo rigen sin la autorización de su titular, será sancionada con pena privativa de libertad de tres a cinco años." (Ministerio de Justicia, Derechos Humanos y Cultos, Subsecretaría de Desarrollo Normativo, 2014)

2.2.2.2 Uso de Reportes Como Respaldo Legal

Es de suma importancia conocer si los reportes emitidos por un sistema informático tienen el aval legal y se puedan utilizar estos reportes o logs como evidencia en el

caso de la existencia de una incidencia. La legislación ecuatoriana menciona que, para la formulación de pruebas o evidencias por parte de un fiscal, se pueden "interpretar datos informáticos que comprueben la presencia de una infracción." (Ministerio de Justicia, Derechos Humanos y Cultos, Subsecretaría de Desarrollo Normativo, 2014) Esto se puede verificar en los artículos 476, 477 y 500 del código orgánico integral penal.

2.2.2.3 Factibilidad Legal

En base que el sistema de detención de intrusos y el módulo Raspberry Pi que se eligieron son Open Source y bajo los principios de sistemas Open Source, los usuarios pueden, "manipular para cambiar la forma en que funciona una pieza, un programa o aplicación." (Red Hat, Inc., 2019) Por lo tanto, no se inflige alguna ley por el uso no autorizado del sistema IDS, ya que no hay que adquirir ningún tipo de licenciamiento, esto aplica de igual forma para el uso del módulo Raspberry Pi, en el caso que se requiera cambiar o agregar algún dispositivo.

CAPÍTULO 3

En este capítulo se tratará, sobre el procedimiento se realizó para implementar y configurar el IDS que se propone como solución, además se explica sobre las configuraciones que se realizaron para simular la red en GNS3.

3.1 Implementación y Configuración de la Solución

3.1.1 Adaptador de Loopback

Para simular una topología PYME real en GNS3 con una conexión a Internet, es necesario que dentro del GNS3 exista una forma para conectar los equipos a Internet, por lo que, se requerirá de una NIC, desde la cual la conexión primaria a Internet puede ser compartida hacia una tarjeta de red o NIC virtual, como se puede apreciar en la figura 13.

Nic Virtual

Figura 10. Creación de NIC Virtual
Elaborado por: Bryan Carate y Francisco Pozo

Esta NIC virtual proveerá una conexión de Internet a la topología en GNS3 y así, simular una conexión a Internet desde el escenario de GNS3 como si se tratara de un ISP, esto se puede apreciar en la figura 14.

Conexión de Internet en GNS3

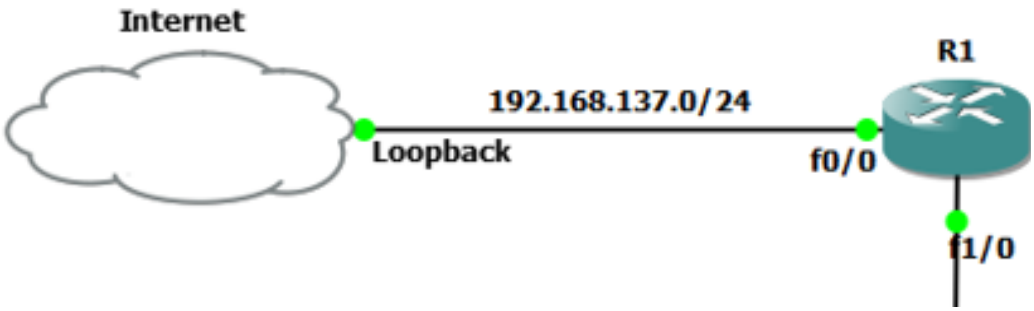

Figura 11. Conexión de internet en GNS3.
Elaborado por: Bryan Carate y Francisco Pozo

El sistema operativo Windows permite instalar una NIC virtual también llamada "Adaptador de bucle invertido de Microsoft", que en este caso será llamada adaptador Loopback, el proceso de instalación de dicho adaptador de Loopback es sencillo, ya que el sistema operativo Windows 7 brinda la facilidad de una interfaz, para instalar el adaptador de Loopback.

3.1.1.1 Pasos Para Instalar un Adaptador de Loopback

Para instalar el adaptador de Loopback se tiene que llamar al Asistente para agregar hardware, como se muestra en la figura 15.

Asistente para agregar Hardware

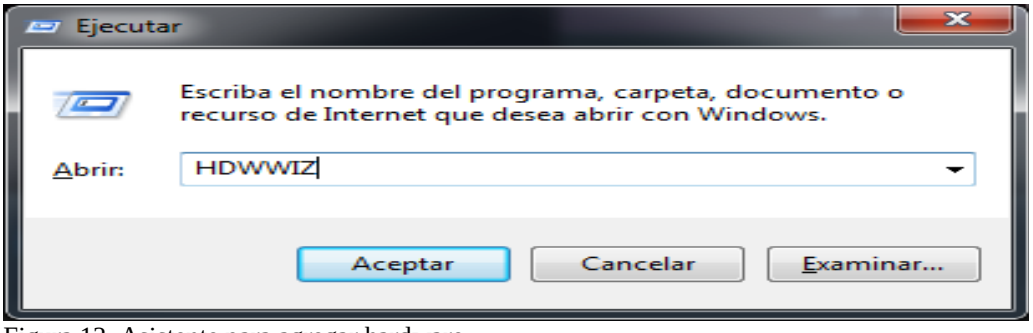

Figura 12. Asistente para agregar hardware
Elaborado por: Bryan Carate y Francisco Pozo

Una vez que inicia el Asistente para agregar hardware, en dicha ventana se explica que esta herramienta permite instalar los controladores para dispositivos no compatibles con la tecnología Plug&Play.

Se selecciona la opción que permite instalar hardware automáticamente, ya que lo que se requiere es un adaptador de Loopback y este vendría a ser una tarjeta de red adicional, se selecciona en la lista de dispositivos la opción de Adaptadores de red.

En la figura 16, se muestran los diferentes fabricantes y el tipo de controlador que se requiere instalar, por lo cual se seleccionara el fabricante Microsoft y el controlador para el Adaptador de bucle invertido de Microsoft.

Tipo de Adaptador de red

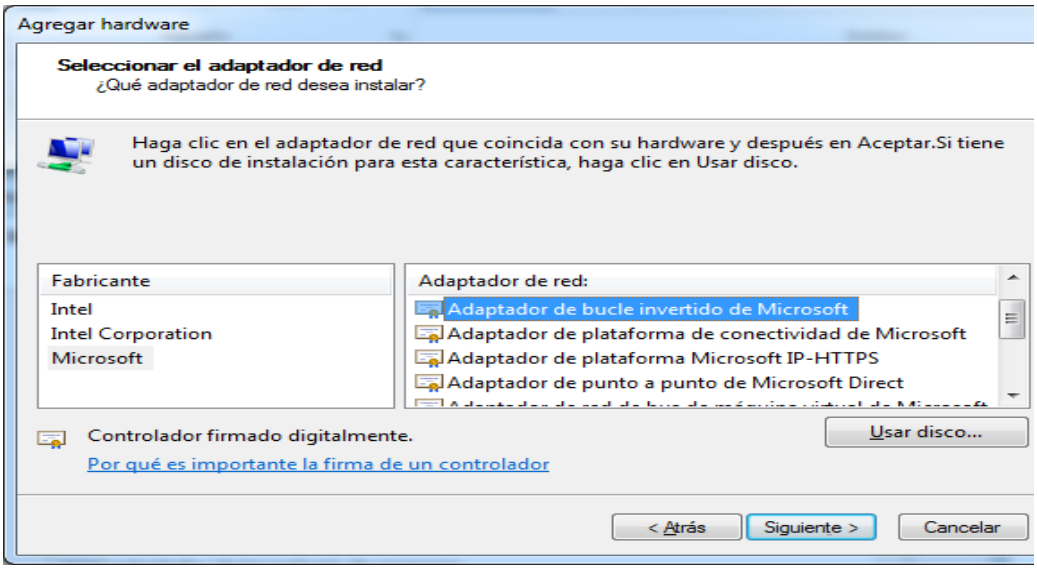

Figura 13. Selección de tipo de adaptador de red
Elaborado por: Bryan Carate y Francisco Pozo

Por último, el Asistente para agregar hardware pide finalizar la instalación y se procede a un reinicio del sistema obteniendo una funcionalidad correcta del nuevo adaptador de Loopback que se instaló.

3.1.1.2 Compartición de Internet de NIC a Loopback

Una vez que el adaptador de Loopback esté instalado, se debe compartir la conexión a Internet desde la NIC física del computador al adaptador de Loopback, este proceso de igual forma se lo realiza dentro del menú de propiedades de la interfaz de red, desde la cual se va a compartir Internet.

Se selecciona la NIC que compartirá Internet, y mediante un clic derecho se ingresa al menú de propiedades, a continuación, se procede a la pestaña de uso compartido en la cual se marca la caja de selección, en la que se indica que la interfaz de red seleccionada va a permitir el uso compartido de Internet a través de esa NIC y se especifica a cuál NIC se compartirá la conexión a Internet, en este caso se seleccionará el adaptador de Loopback, como se muestra en la Figura 17.

Compartición de Internet NIC a Loopback

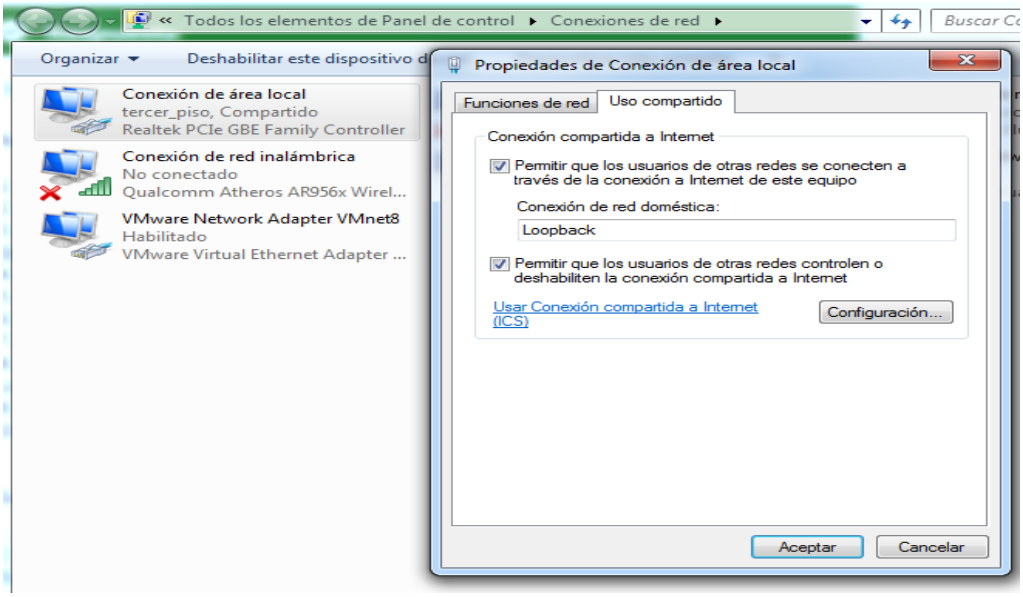

Figura 14. Compartición de internet NIC a Loopback
Elaborado por: Bryan Carate y Francisco Pozo

3.1.2 **Configuración de IOS de Cisco**

La familia del Router que se simula es parte de los Cisco 3600, la IOS que se utiliza es la que se muestra en la figura 18, una IOS de Cisco es el sistema operativo propietario de Cisco con el cual trabaja la mayoría de sus dispositivos.

IOS Cisco c3600

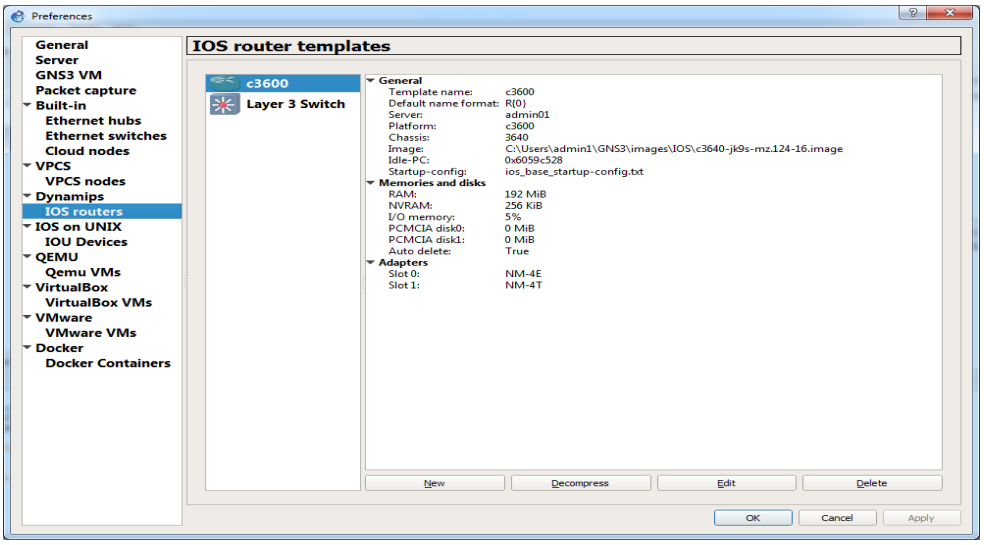

Figura 15. Configuración de IOS Cisco c3600
Elaborado por: Bryan Carate y Francisco Pozo

Dentro de la opción de preferencias de GNS3 y en la pestaña de Dynamips, se agregan dispositivos con IOS específicas o equipos con configuraciones personalizadas, Dynamips es un programa que emula equipos Cisco; y el cual funciona con imágenes reales del sistema operativo de los equipos mencionados.

Se agrega la IOS del Router c3600, mencionado anteriormente, con la configuración exclusiva solo de Router y; adicionalmente, se agrega otro con la excepción que se marca el casillero en donde menciona que el equipo tiene funcionalidades de Switch.

3.1.2.1 Configuración de Salida a Internet

Una vez configurado el acceso a Internet al adaptador de Loopback, dentro del GNS3 se coloca una nube, esta nube dentro de sus configuraciones tiene disponible todas las interfaces de red útiles, como se muestra en la figura 19.

Salida a Internet

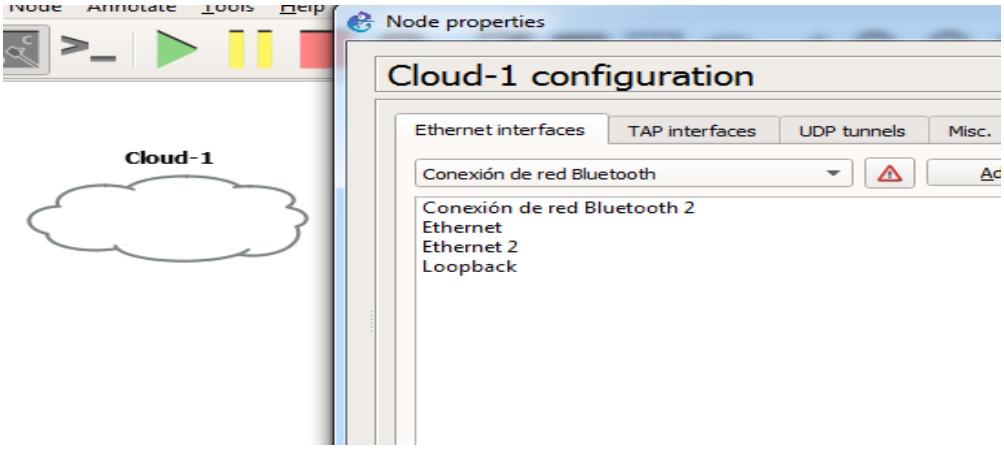

Figura 16. Configuración de salida a internet en GNS3
Elaborado por: Bryan Carate y Francisco Pozo

Esta conexión simula el lugar de un ISP, el cual brinda acceso a Internet a los dispositivos que se les realice la configuración dentro de GNS3. R1 simula un Router brindado por el proveedor de Internet y su función es de puerta de enlace hacia la red externa, por donde el tráfico de los dispositivos transita hacia Internet.

Para que la red local dentro de GNS3 se conecte a Internet, se realiza una conexión en la cual se elige la interfaz de Loopback en la nube representando Internet, mostrado en la figura 20.

Conexión a la Loopback

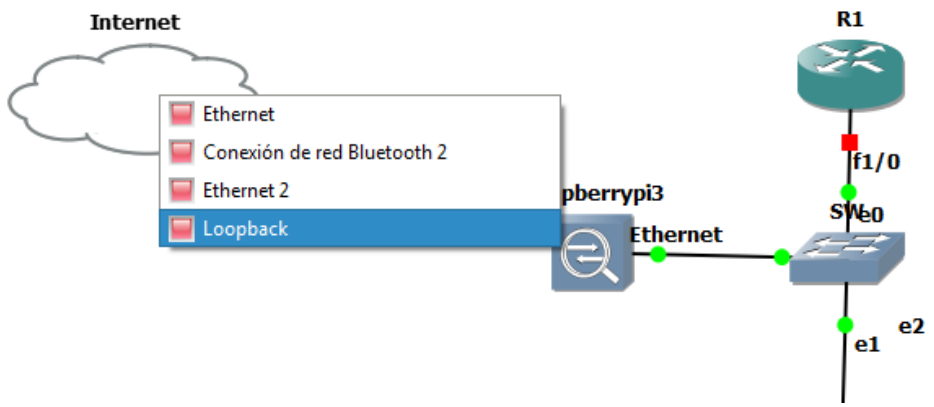

Figura 17. Conexión de GNS3 a la Loopback
Elaborado por: Bryan Carate y Francisco Pozo

Mientras que al otro extremo de la conexión se selecciona una interfaz del Router R1, a partir de este punto se procede con diseño de la red PYME.

3.1.3 **Diseño de Topología de Red PYME**

Al ser el diseño de una red PYME, se intenta replicar una red en producción, apegada a la realidad de una pequeña o mediana empresa en el Ecuador. El diseño consta de un ISP, el cual vendría a ser la nube que simula Internet, un Router que es proveído por el ISP, un Switch conectado a un puerto del Router y a este el resto de dispositivos que se tengan conectados a la red, el IDS y los usuarios. Esto se puede apreciar en la figura 21.

Topología de red PYMES

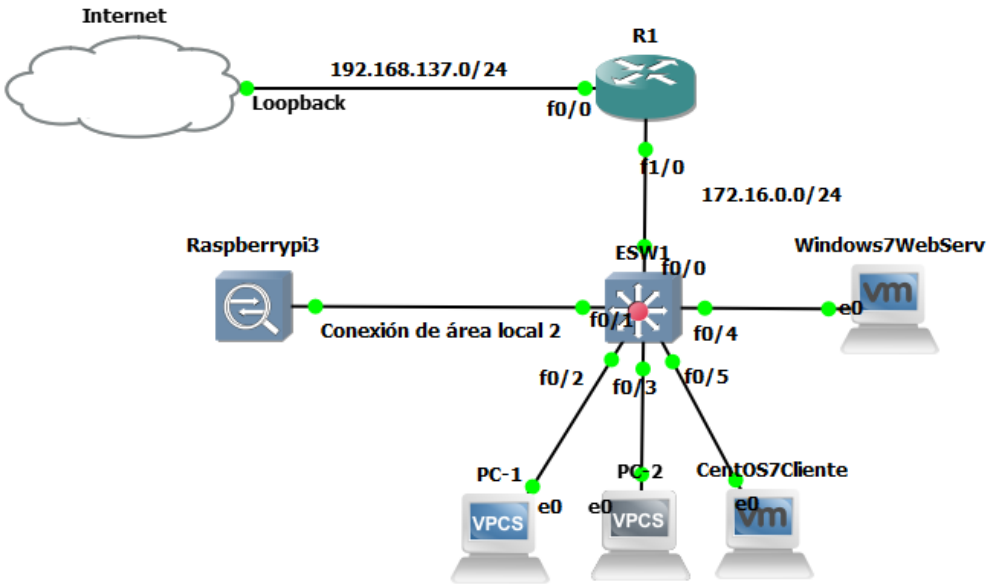

Figura 18. Topología de red
Elaborado por: Bryan Carate y Francisco Pozo

Ya que la nube simula ser el ISP, en otras palabras, un segmento WAN, este segmento tiene un rango de IP diferente al de la red LAN, en la interfaz f 0/0 el Router tiene una configuración para que reciba una IP mediante DHCP y en la interfaz f 1/0 se configura la red LAN.

3.1.4 **Configuración de DNS en el Router**

Ya que el adaptador de Loopback es la que simula la conexión a Internet en la topología dentro de GNS3, dicho adaptador debe ser apuntado para que resuelva las peticiones de DNS, se debe tomar en cuenta, qué IP está siendo asignada al adaptador de Loopback, en este caso es la 192.168.137.1/24, por lo tanto, esa será la IP asignada para que resuelva peticiones DNS, como se muestra en la figura 22.

Comandos de configuración de DNS

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-lookup
R1(config)#ip name-server 192.168.137.1
R1(config)#end
```

Figura 19. Comandos de configuración de DNS
Elaborado por: Bryan Carate y Francisco Pozo

3.1.5 **Configuración de NAT Para la Comunicación Entre Interfaces**

La configuración NAT permite que cuando los usuarios soliciten conexión a Internet, el Router envié todo el tráfico a través de su IP, en este caso la 192.168.137.1. Cuando esta información regrese hacia los usuarios, el Router direcciona dicha información a su respectivo destino.

Para que haya una conexión a Internet desde la red interna 172.16.0.0/24 hacia Internet, el tráfico de la interfaz f 1/0 debe salir por la interfaz f 0/0 a través de la IP 192.168.137.1/24 de la red externa, esto se lo realiza mediante una configuración NAT, a través de los siguientes comandos. Se puede destacar que en cada configuración respectiva en la interfaz del Router se menciona cuál es su posición en la configuración NAT, sea esta externa como el caso de f 0/0, o interna como el caso de f 1/0. Adicionalmente, en la última línea de comandos se indica que la IP asignada a f 0/0 pueda ser usada para una conexión concurrente, desde múltiples clientes de la red interna para que puedan tener una comunicación hacia la red externa.

Por último, se especifica que todas las IP de la red 172.16.0.0/24 serán traducidas hacia la red externa.

3.1.6 **Configuración de Puertos del Switch**

Ya que el módulo Raspberry realizará un monitoreo del tráfico, se debe configurar Port Mirroring en el Switch, para que se realice un espejo del tráfico desde uno o varios puertos, en específico hacia un puerto destino, se tiene que ingresar a la configuración global del Switch, e indicar si el puerto es una fuente de tráfico, o el destino donde se refleja todo el tráfico; para ser monitorizado.

Las interfaces: f 0/0, f 0/2 y f 0/3, son la fuente del tráfico, a medida que se requiera, se pueden agregar más puertos como fuentes de tráfico, la línea de comandos es la misma para cualquier puerto que se desee monitorizar, solo se debe especificar qué puerto se requiere monitorear.

Se especifica que la interfaz f 0/1 del Switch, será configurado como puerto destino, es decir, se realizará un espejo o copia del tráfico de los anteriores puertos especificados, y se enviará a este puerto en particular, para que el Raspberry analice estos datos.

3.1.7 **Configuración de Raspberry PI 3**

El sistema operativo que se seleccionó, es Raspbian Lite (Stretch), instalado mediante NOOBS, NOOBS es un aplicativo Software libre, que facilita una lista de varios sistemas operativos en la cual se puede escoger el que más se acomode al requerimiento del usuario, basta seleccionar el OS, en este caso Raspbian Lite y presionar el botón Install, como se muestra en la figura 23. Se debe tomar en cuenta que previamente el módulo Raspberry debe tener una conexión a Internet para que pueda descargar automáticamente paquetes adicionales requeridos para la instalación del OS.

Raspbian Lite (Stretch)

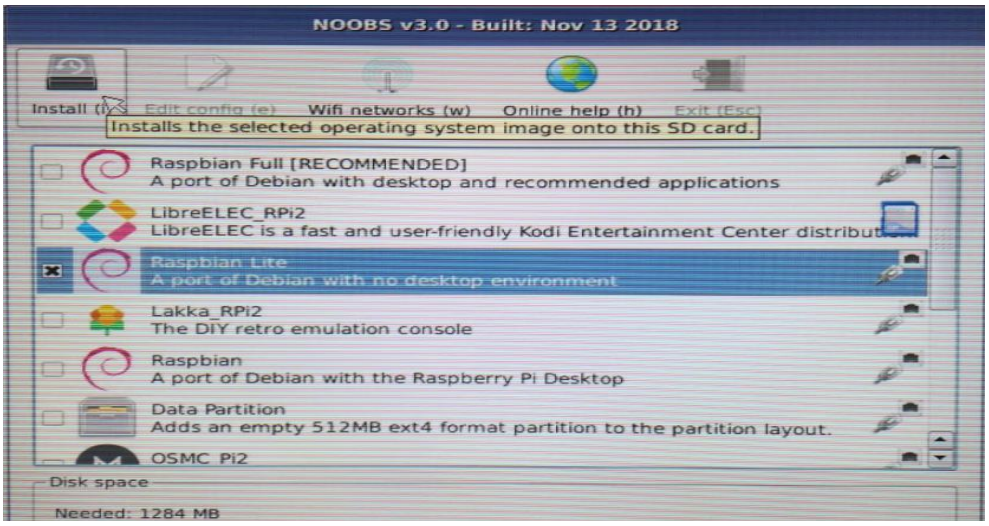

Figura 20. Instalación de Raspbian lite
Elaborado por: Bryan Carate y Francisco Pozo

El instalador muestra una alerta que anuncia que toda la información en la tarjeta SD se eliminará, se presiona “SI” para continuar.

Una vez termina la instalación es necesario hacer la configuración de contraseña de usuario root, el usuario que tiene instalado por defecto, por parte del sistema operativo: es ‘pi’ con contraseña ‘Raspberry’. El primer paso que se cumple, es configurar la contraseña del usuario ‘root’, para evitar problemas en el momento que se requiera realizar acciones con permisos elevados, el sistema solicitará la contraseña del usuario ‘root’, en este caso la contraseña es ‘root’.

3.1.7.1 Activación de Servicio SSH del Módulo Raspberry

Ya que en el primer ingreso a las configuraciones del módulo Raspberry se hace mediante un monitor, un mouse, la conexión a Internet de la red LAN del computador y un teclado, una conexión remota mediante SSH facilitará el acceso a la línea de comandos del sistema operativo, de tal forma que se habilita este servicio para continuar con las configuraciones.

Para realizar una conexión remota al Raspberry, previamente se debe conocer que IP fue asignada desde el Router de la red LAN del computador, una vez que se conozca esto, mediante 'PuTTY' es una opción por la cual se puede acceder al módulo Raspberry.

3.1.7.2 Descarga del Código Fuente y el Paquete de Dependencia DAQ

Los paquetes de instalación del IDS se pueden descargar directamente desde la página de 'Snort', en dicha página se muestra los diferentes enlaces para su respectiva descarga según el OS que se requiera, como se muestra en la siguiente figura 24.

Código fuente y paquete DAQ

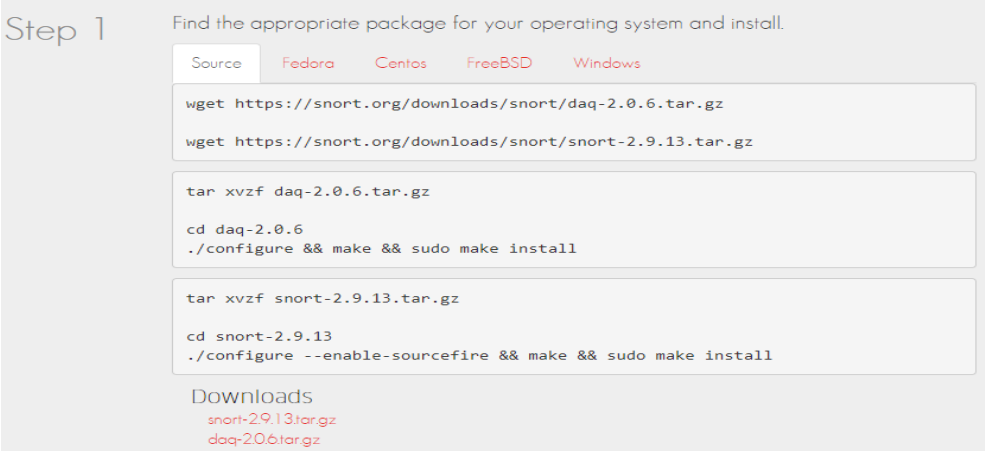

Figura 21. Código fuente y paquete DAQ
Elaborado por: Bryan Carate y Francisco Pozo

Se puede apreciar que existen dos enlaces, el primero con las siglas en inglés 'DAQ' que representa el 'tarball' de adquisición de datos, la cual es una serie de comandos que son necesarios para que 'Snort' funcione correctamente y el segundo enlace que contiene el 'tarball' del código fuente de 'Snort'.

3.1.7.3 Instalación de Snort

La instalación de ‘Snort’ es similar a la instalación de la dependencia ‘DAQ’, ya que se tienen descargados ambos paquetes, primero se instala las dependencias ‘DAQ’ y una vez que los requerimientos se cumplan se procede a instalar el sistema de detección de intrusos.

3.1.7.4 Reglas de Snort

Una vez que se validó las configuraciones básicas, se puede empezar a configurar el archivo de las reglas.

La sintaxis de las reglas se puede apreciar en la figura 25.

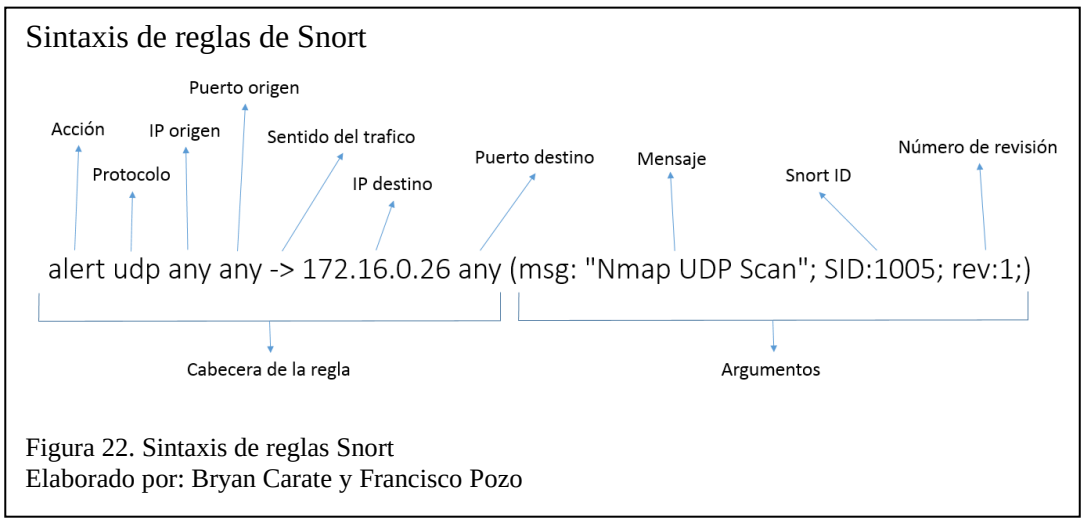

Figura 22. Sintaxis de reglas Snort
Elaborado por: Bryan Carate y Francisco Pozo

En este archivo se asignan seis reglas, cada regla tiene un ‘SID’ o identificación de ‘Snort’ las cuales se las ha asignado en el rango del 1001 hasta el 1006 y vinculado al conjunto de reglas ‘rev:1’. A continuación, se realizará una explicación de cada regla por individual haciendo referencia a su ’SID’:

- (SID:1000000001) Esta regla emite una alerta sobre cualquier petición HTTP desde cualquier red ya sea interna o externa a través del puerto 8080 a la IP 172.16.0.26, en esta IP se simula un servidor WEB.

- (SID:1000000002) Esta regla emite una alerta sobre cualquier tráfico ICMP hacia cualquier puerto dentro de la red interna.
- (SID:1000000003) Esta regla emite una alerta sobre cualquier tipo de escaneo 'XMAS' mediante NMAP a la IP 172.16.0.26 en el puerto 22 desde cualquier red, adicionalmente usa un parámetro en el cual se indica la bandera de la cabecera, en este caso la bandera 'FPU'.
- (SID:1000000004) Esta regla emite una alerta sobre cualquier tipo de escaneo 'FIN' mediante NMAP a la IP 172.16.0.26 en el puerto 22 desde cualquier red, adicionalmente usa un parámetro en el cual se indica la bandera de la cabecera, en este caso la bandera 'F'.
- (SID:1000000005) Esta regla emite una alerta sobre cualquier tráfico UDP hacia la IP 172.16.0.26 en cualquier puerto desde cualquier red.
- (SID:1000000006) Esta regla emite una alerta sobre cualquier tráfico ICMP desde la red interna hacia la red externa a través de cualquier puerto.

3.1.7.5 Integración del Módulo Raspberry PI 3 con la Topología en GNS3

Todas estas previas configuraciones se las realizó con una conexión desde la red LAN del computador separado de la simulación que se realizará, ya que todas las configuraciones se las realizó con éxito finalmente se debe integrar el módulo Raspberry con la topología PYME en GNS3.

Simplemente se asigna una IP estática en este caso la IP 172.16.0.3/24 y se configura la puerta de enlace de la red interna en GNS3 que vendría a ser la IP 172.16.0.1/24, para que todos estos cambios tomen efecto se reinicia el módulo Raspberry con el comando de la figura 26.

Reinicio de Raspberry

```
[pi@localhost]$ sudo reboot
```

Figura 23, comando para reiniciar Raspberry
Elaborado por: Bryan Carate y Francisco Pozo

Para que el módulo Raspberry se conecte con la topología en GNS3 se vinculó un conector USB-Ethernet al computador y este conector conectado directamente el puerto Ethernet del módulo Raspberry, como se muestra en la figura 27.

Conexión del módulo Raspberry con la topología en GNS3

Figura 24. Conexión del módulo Raspberry con la topología en GNS3
Elaborado por: Bryan Carate y Francisco Pozo

Dentro de la topología de GNS3, se agregó una nube, la cual se le cambio el icono a un analizador de paquetes, este vendría a ser el módulo Raspberry que se encuentra trabajando como IDS, por último, se realiza una conexión entre el puerto f 0/1 del 'Switch' y la interfaz "conexión de área local 2" en el dispositivo que se agregó.

Topología de red

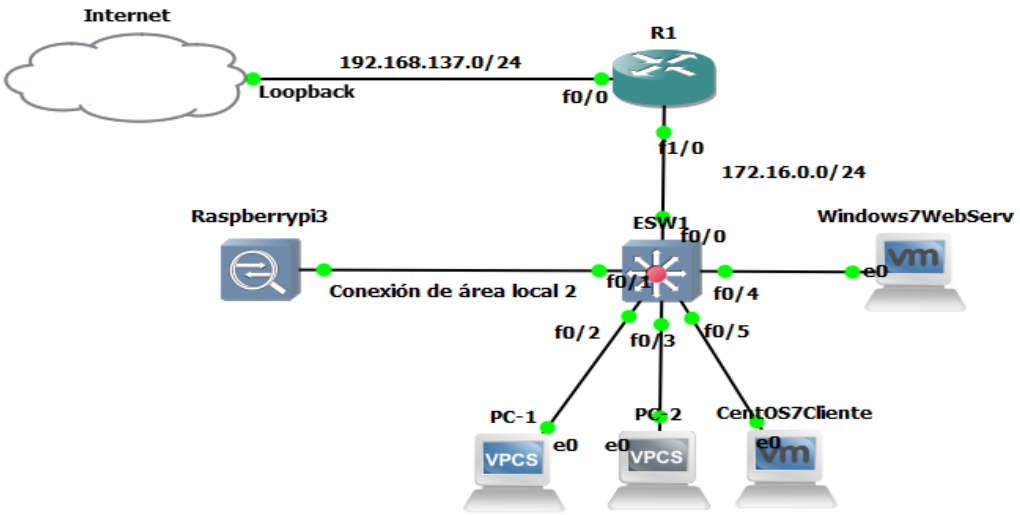

Figura 25. Topología de red final
Elaborado por: Bryan Carate y Francisco Pozo

En la figura 28, se puede ver cuál es el diseño de red final que simulará una PYME.

CAPÍTULO 4

En este capítulo se tratará, sobre el procedimiento se realizó para evaluar el sistema de detección de intrusos, el tipo de pruebas, las estadísticas que emitieron los resultados de las pruebas, y por último la efectividad y eficiencia del IDS.

4.1 Pruebas y Resultados de la Implementación

4.1.1 Análisis de las Pruebas de la Implementación

En la configuración del IDS se crearon reglas como se explicó en la sección 3.1.7.4, las cuales permiten identificar un comportamiento específico en la red, catalogado como anómalo. Se realiza la evaluación del IDS mediante dos tipos de ataques: DoS, el cual intenta saturar la red con tráfico, para anular la comunicación entre dispositivos o servicios y Probing, el cual realiza un escaneo para determinar vulnerabilidades, los cuales pueden ser usados posteriormente para comprometer a un sistema.

4.1.2 Evaluación de Efectividad

La habilidad para que el IDS detecte ataques y el porcentaje de falsas alarmas. Un sistema de detección de intrusos debe ser capaz de emitir alarmas cuando ocurra una incidencia, mientras que la tasa de falsas alarmas se mantenga a un nivel mínimo. La tasa de detección de ataques debería ser de 1 y la tasa de falsa alarma debe ser 0.

Para evaluar la efectividad del IDS, se plantearon pruebas en las cuales, se emite flujo de dos tipos de tráfico en la red, de tal manera que, se pueda determinar si el sistema es capaz de detectar todo el tráfico catalogado como un ataque.

4.1.2.1 Prueba de Ataque Distribuido

Se realizó un ataque distribuido para medir la efectividad del IDS en un rango de 7 segundos, se efectuó 5 ataques desde 3 hosts simultáneamente, de estos 15 ataques se obtuvo un acierto del 100%, en la gráfica 29, se puede apreciar que durante el tiempo 37:29 hasta el 37:32 se detecta la sincronización de los ataques, cada ataque duro un aproximado de 4007.66 ms

Ataque Distribuido

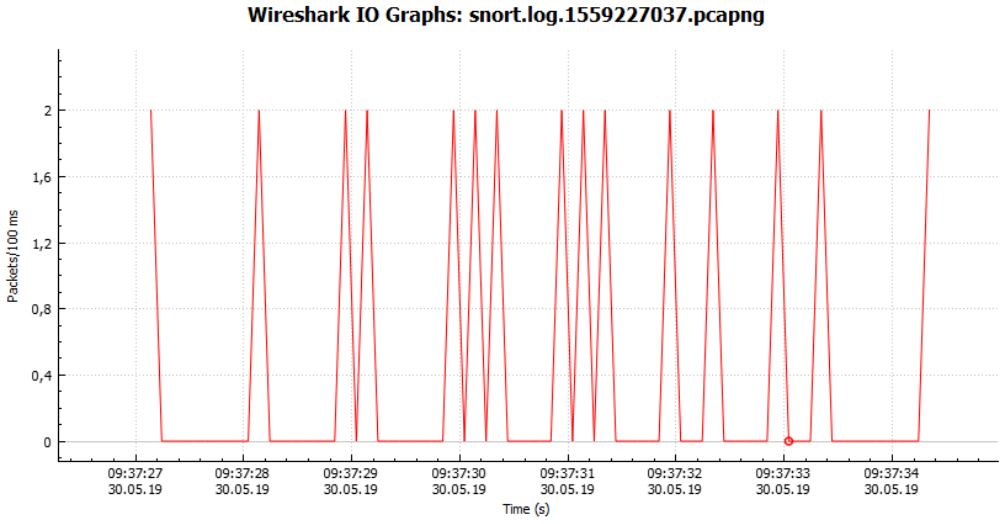

Figura 26. Gráfica de un ataque distribuido
Elaborado por: Bryan Carate y Francisco Pozo

En la figura 30, con el archivo .PCAP que el IDS genera posterior al finalizar el servicio de detección de intrusos. Mediante la herramienta en línea Packettotal, se puede analizar este archivo y apreciar mejor el pico donde se tuvieron el mayor flujo de incidencias simultáneas.

Packettotal

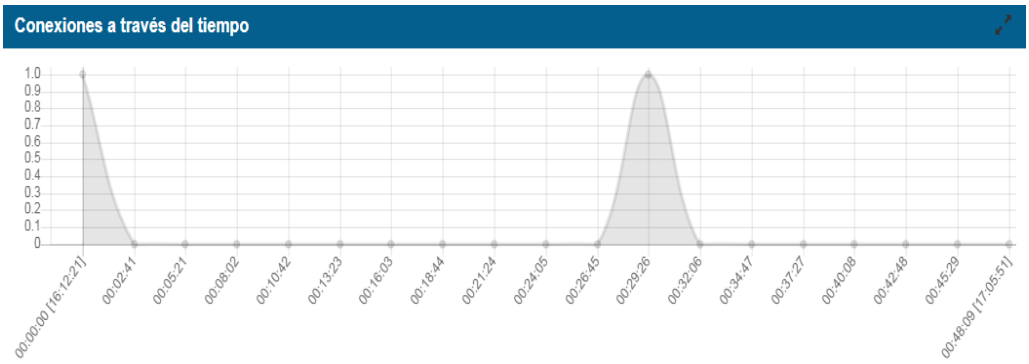

Figura 27. Gráfica de conexión a través del tiempo
Elaborado por: Bryan Carate y Francisco Pozo

Se puede observar que hay una detección elevada durante un tiempo estimado de 5 segundos donde la gráfica muestra un incremento de un cierto tipo de incidencias.

En la figura 31, se puede apreciar que todas las conexiones se detectaron con éxito. Como se describió en la sección 4.2 la eficiencia debe acercarse a 1, así evidenciando que en esta prueba existe una tasa de eficiencia del 100%.

Efectividad

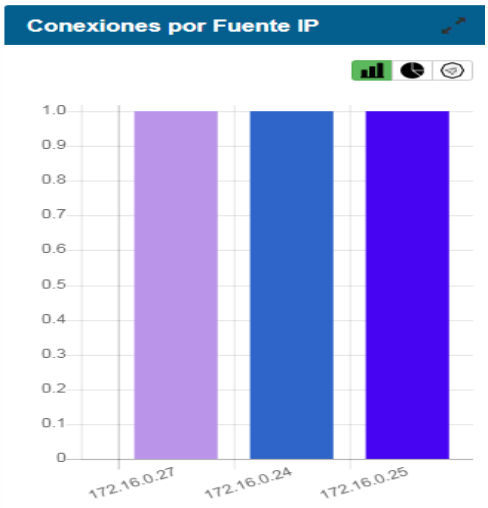

Figura 28. Gráfica de efectividad
Elaborado por: Bryan Carate y Francisco Pozo

4.1.2.2 Prueba de Ataque Secuencial

La evaluación se constituye de 5 pruebas, que radican en el flujo de dos tipos de tráfico secuencialmente, y determinar si se detectan todas las amenazas. Se analizará si el IDS detecta cada prueba frente a la cantidad de veces que se lanzó el ataque.

En la figura 32, se puede apreciar los comandos que se ejecutaron para los dos tipos de tráfico que se emiten desde el cliente CentOS a través del terminal.

Comandos para generar Tráfico

```
[root@localhost clientecentos]# nmap -sX -p22 172.16.0.26

Starting Nmap 6.40 ( http://nmap.org ) at 2019-05-22 01:11 ECT
Nmap scan report for 172.16.0.26
Host is up (0.00052s latency).
PORT   STATE  SERVICE
22/tcp closed ssh
MAC Address: 00:0C:29:39:23:23 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
[root@localhost clientecentos]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=101 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=95.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=101 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=95.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=99.9 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 95.083/98.769/101.594/2.734 ms
[root@localhost clientecentos]#
```

Figura 29. Comandos para generar tráfico
Elaborado por: Bryan Carate y Francisco Pozo

4.1.2.3 Análisis de Curva ROC

Para evaluar la precisión en la detección de falsos positivos, es necesario el uso de la curva ROC–AUC, para distinguir entre amenazas y no amenazas. En el desarrollo de la curva ROC se hace uso del programa “Metz ROC Software” de la Universidad de Chicago, la figura 33, se muestran los valores tomados de las cinco pruebas para desarrollar la curca ROC.

Curva ROC

Prueba	Frecuencias observadas		Tasas acumuladas	
	No resuelto	Analizado	Falso positivo	Verdadero Positivo
1	3	127	0.1579	0.1689
2	3	129	0.3158	0.3404
3	3	135	0.4737	0.5199
4	5	139	0.7368	0.7048
5	5	222	1	1

Figura 30. Resultados de la curva ROC
Elaborado por: Bryan Carate y Francisco Pozo

La ecuación propuesta por el programa "Metz ROC Software" para generar los datos de la curva, es la que se muestra en la figura 34, en esta figura se aprecia de igual forma el área bajo la curva.

Ecuación de curva ROC

Curva ROC para $y = 0.5\ln(x) + 0.94$
Área bajo la curva= 0.4512

Figura 31. Ecuación de la curva ROC
Elaborado por: Bryan Carate y Francisco Pozo

Se puede observar la tendencia de la curva en la figura 35, mostrando el comportamiento frente a una incidencia.

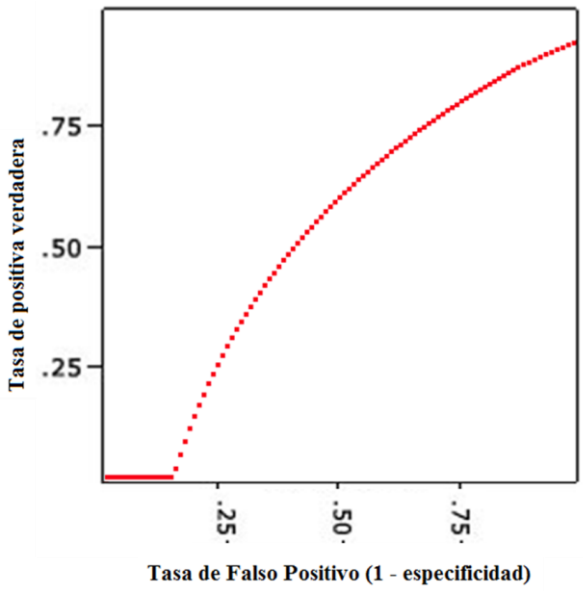

Figura 32. Porcentaje de falso positivo
Elaborado por: Bryan Carate y Francisco Pozo

Evidenciando que, en esta prueba mientras inicializó el ataque hubo paquetes que no se analizaron entregando falsos positivos, esto se debe a que no se le dio un tiempo para que el sistema se estabilice bien, la taza de paquetes analizados empezó a incrementar mientras continúa la prueba.

4.1.3 **Pruebas de Ataque Simultáneo**

En la prueba de ataques simultáneos, se emitió los dos tipos de tráfico a la vez, en la figura 36, se puede observar las estadísticas de la prueba.

Estadística de ataques simultáneos

Prueba ataques simultáneos		
Total recibidos	4060	
Analizados	4055	99,877%
No resuelto	5	0,123%
Tiempo (s)	291,26875	
Pkts/s	13	

Estadísticas por protocolo	No. Pkts	%			
Eth	4058	100,000%			
IP4	2415	59,512%			
ICMP	1374	33,859%			
UDP	71	1,750%			
TCP	970	23,903%			
ARP	1336	32,923%			
Eth Loop	14	0,345%			
Other	258	6,358%			
Bad Chk Sum	666	16,412%	IP6	35	0,862%
IP6 packets	95	2,341%	IP6 EXT	35	0,862%
			UDP6	25	0,616%

Figura 33. Estadística de ataques simultáneos
Elaborado por: Bryan Carate y Francisco Pozo

En la figura 37, se puede apreciar la taza de paquetes analizados y los no resueltos, esta evaluación dio una tasa del 99,877% de paquetes analizados y una tasa del 0,123% de paquetes no analizados.

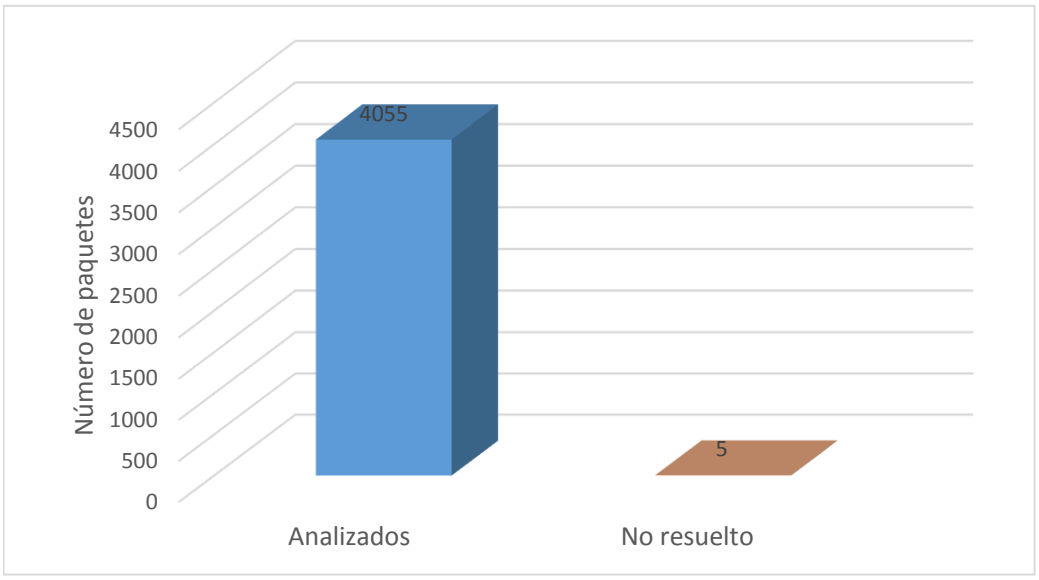

Figura 34. Porcentaje de paquetes analizados
Elaborado por: Bryan Carate y Francisco Pozo

La efectividad de análisis del IDS en esta prueba es del 99,877% y una tasa de paquetes no analizados del 0,123%.

De estas pruebas, se puede obtener un porcentaje de paquetes según el protocolo que se transmitió, los cuales se pueden apreciar en la figura 38.

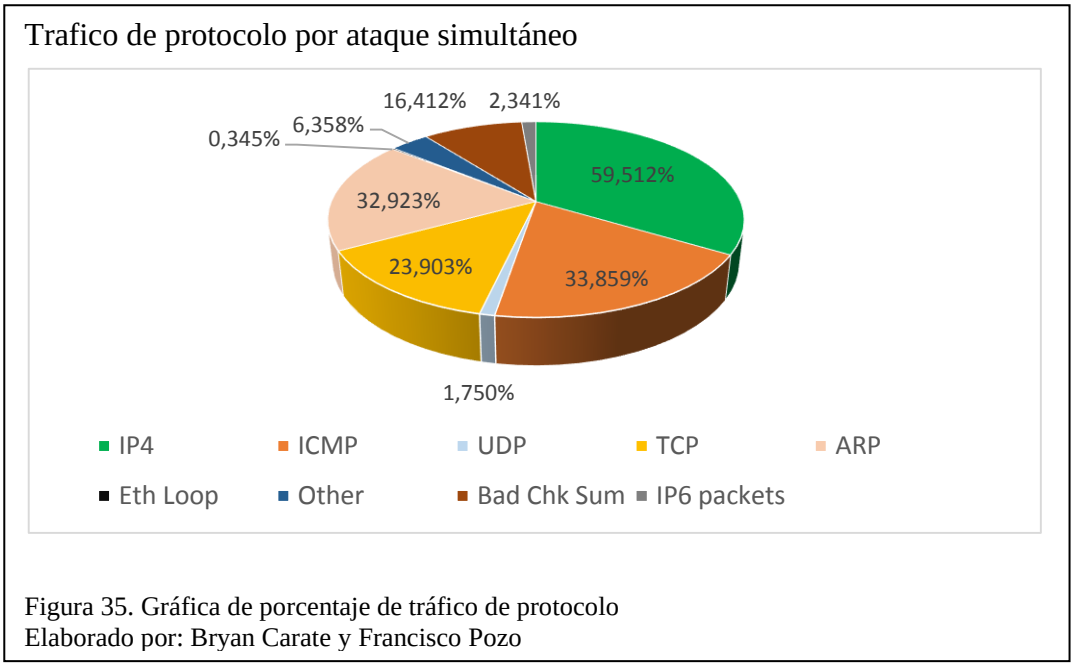

Figura 35. Gráfica de porcentaje de tráfico de protocolo
Elaborado por: Bryan Carate y Francisco Pozo

4.1.4 **Promedio de Efectividad de las Pruebas**

Para evaluar la efectividad de las pruebas de intrusión, se obtiene una media de la sumatoria de los resultados de las pruebas, como se muestra en la tabla 18.

Tabla 18. Promedio de efectividad

Prueba	Paquetes Analizados	Paquetes No Resueltos
1	0,976923077	0,165287294
2	0,977272727	0,023076923
3	0,97826087	0,022727273
4	0,965277778	0,02173913
5	0,977973568	0,034722222
6	0,998768473	0,022026432
7	0,834712706	0,001233046
8	0,993047509	0,007001167
9	0,99905303	0,000947867
10	0,986149584	0,014044944
Total	9,687439322	0,312806298
Promedio	96,87%	3,13%

Elaborado por: Bryan Carate y Francisco Pozo

El IDS a través estas pruebas ha demostrado que tiene una efectividad de paquetes analizados del 96,87% y un promedio de 3,13% de paquetes no resueltos.

4.1.5 **Pruebas de Ataque Prolongado**

Se realiza una prueba donde se inicializa el IDS por un tiempo prolongado de 9 horas aproximadamente, realizando pruebas secuenciales eventuales y monitorizando el comportamiento de la red. En la figura 39, se puede apreciar las estadísticas del análisis.

Estadística de análisis prolongado

Prueba ataques simultáneos		
Total recibidos	5354368	
Analizados	4469359	83,471%
No resuelto	885009	16,529%
Tiempo (s)	32.400,14331	
Pkts/s	137	

Estadísticas por protocolo	**No. Pkts**	**%**
Eth	4469449	100,000%
IP4	1383821	30,962%
ICMP	90439	2,023%
UDP	302826	6,775%
TCP	990310	22,157%
ARP	397189	8,887%
Eth Loop	3106	0,069%
Other	52540	1,176%
Bad Chk Sum	31065	0,695%
IP6	2633039	58,912%
IP6 EXT	2633284	58,917%
IP6 Opts	245	0,005%
ICMP6	111687	2,499%
UDP6	2492290	55,763%
TCP6	29062	0,650%
ICMP-IP	68388	1,530%

Figura 36. Estadística de análisis prolongado
Elaborado por: Bryan Carate y Francisco Pozo

Se evalúa que el porcentaje de efectividad del IDS es del 83,471% y el porcentaje de fallo es del 16.529%. Como se puede observar en la figura 40.

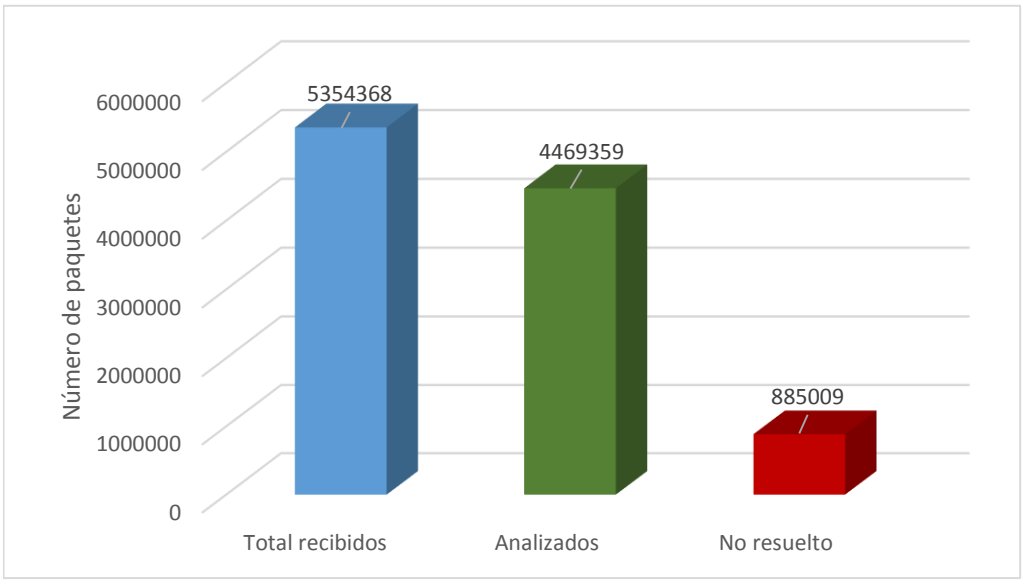

Figura 37. Porcentaje de efectividad de un ataque prolongado
Elaborado por: Bryan Carate y Francisco Pozo

De estas pruebas, se puede obtener un porcentaje de paquetes según el protocolo que se transmitió, los cuales se pueden apreciar en la figura 41.

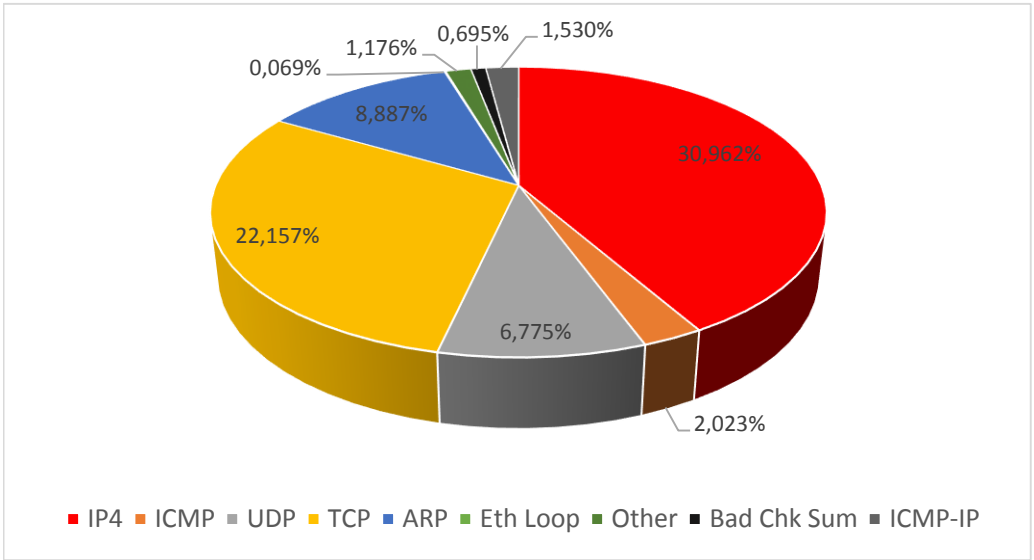

Figura 38. Gráfica de porcentaje de paquetes
Elaborado por: Bryan Carate y Francisco Pozo

4.1.6 **Análisis de LOG Emitido por el IDS**

Con el analizador de archivos en línea tipo ".PCAP", "Packettotal", se examinó los logs emitidos por el IDS, proporcionando una interpretación grafica de los datos recopilados, como el número de conexiones a través del tiempo, el número de conexiones por destino IP y el número de conexiones por puerto destino.

Las conexiones a través del tiempo están representadas en la figura 42.

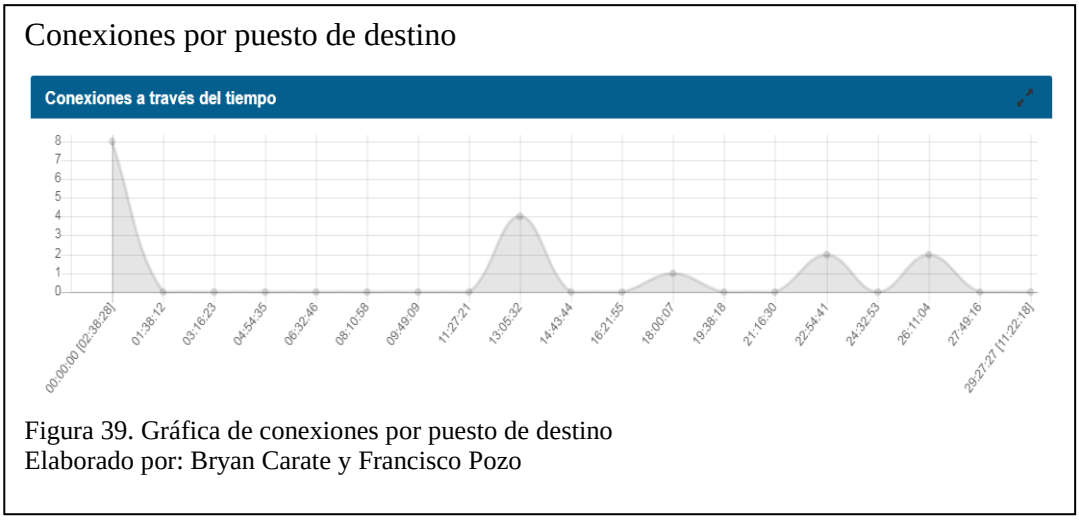

Figura 39. Gráfica de conexiones por puesto de destino
Elaborado por: Bryan Carate y Francisco Pozo

Se puede apreciar que al inicio de la evaluación se detectó los ataques que se realizaron, hubo un lapso que no ocurrió ninguna alerta y se volvieron a realizar ataques.

El mayor número de conexiones realizadas hacia una dirección IP fueron hacia el DNS público de Google, esto se puede apreciar en la figura 43.

Número de Conexiones realizadas

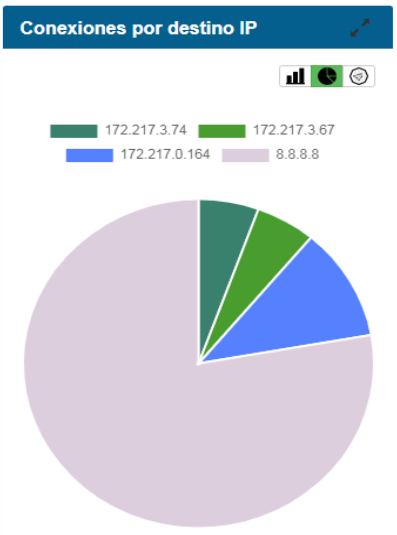

Figura 40. Gráfica de número de conexiones
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7 **Evaluación de Eficiencia**

Un IDS debe consumir menos tiempo y memoria para detectar intrusiones, a la vez de emitir alertas. La funcionalidad de un sistemas de detección de intrusos es la brindar seguridad y de únicamente detectar intrusiones a nivel de red, como es el caso de NIDS. Si el IDS demanda una gran cantidad de uso del CPU, el resto de recursos serán ineficientes para brindar un servicio de seguridad al resto de usuarios.

4.1.7.1 Estado del CPU Inicial Previo al Inicio del IDS

Antes de inicializar el IDS, mediante el software HTOP se ha tomado una muestra de la carga en el procesador y memoria en el módulo Raspberry, antes de ejecutar el servicio de IDS y se muestra un uso del CPU del 1.3%, como se puede ver en la figura 44.

Carga en el Procesador

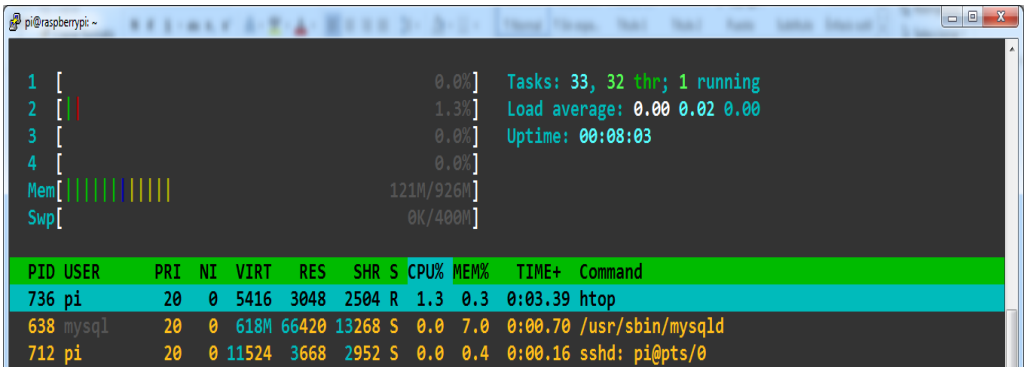

Figura 41. Estado de carga en el procesador antes de iniciar el IDS
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7.2 Estado al Inicializar el IDS

Al iniciar el servicio del IDS también se realiza una medición del rendimiento del CPU, en el cual se observa que se exige una gran cantidad de procesamiento, según las estadísticas que muestra HTOP, se exige el 100% al procesador, pero tiene un consumo de memoria del 8,6%, este proceso de inicialización dura aproximadamente 1 minuto con 9,06 segundos, con esto se indica cual es el estado del CPU antes de inicializar el IDS.

Rendimiento del CPU

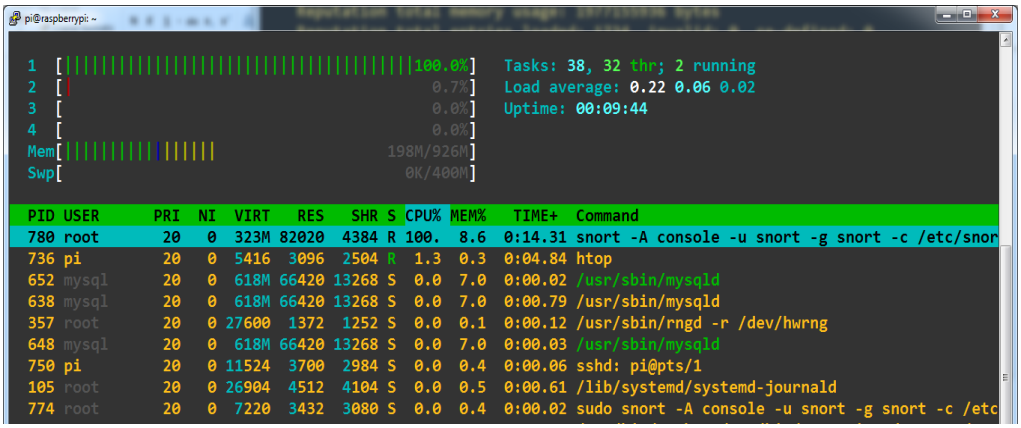

Figura 42. Rendimiento del CPU antes de inicializar el IDS
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7.3 Estado Previo a la Detección de Ataques

Una vez que el IDS inicializa y está listo para detectar amenazas, se vuelve a medir el rendimiento del módulo Raspberry, y muestra que se estabilizó y se encuentra en un uso del CPU del 1.3% y en memoria RAM exige el 25,9%, como se muestra en la figura 46.

IDS inicializado

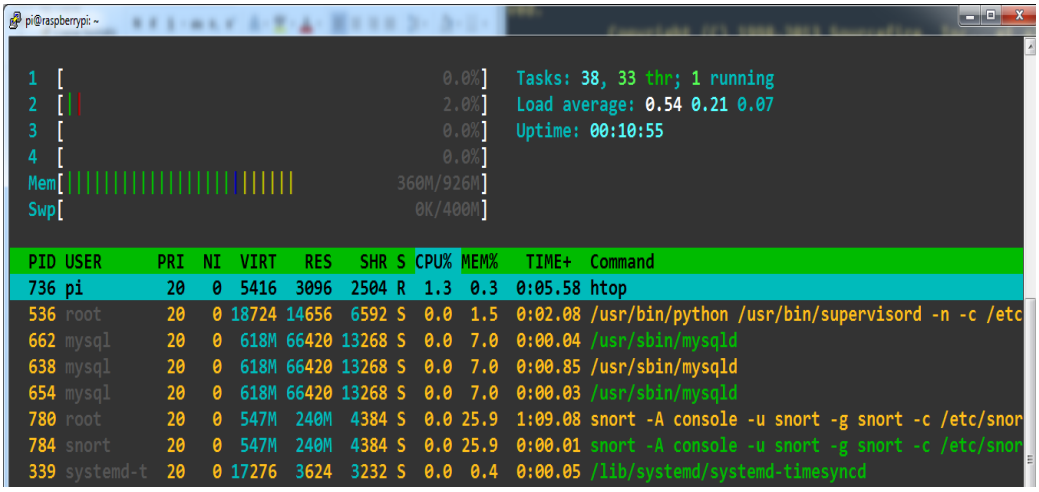

Figura 43. Rendimiento del CPU inicializado el IDS
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7.4 Durante 20 Ataques Secuenciales

Se realizaron 20 ataques secuenciales para observar el rendimiento del IDS ante ataques, donde se aprecia que el uso del CPU no ha variado, a pesar de que se ha detectado en un 100% los ataques realizados, el uso de memoria RAM sigue constante desde que se inicializó los servicios de IDS.

Ataque secuenciales

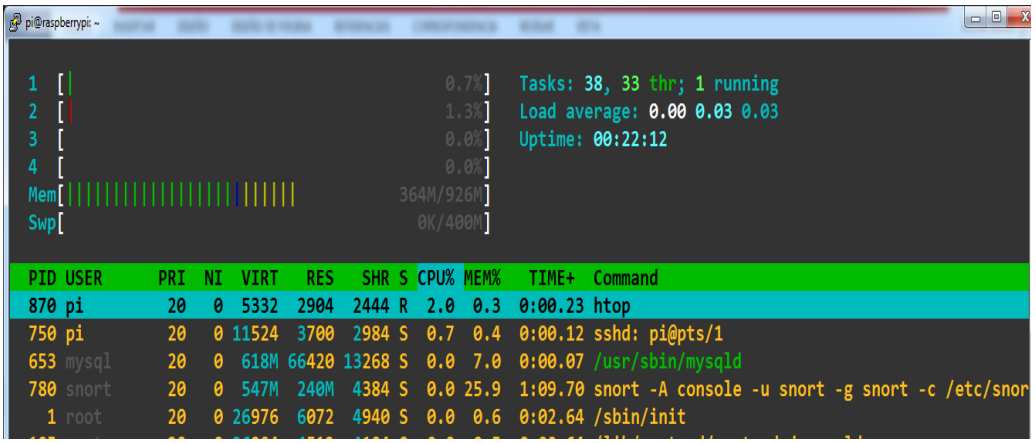

Figura 44. Rendimiento del IDS y del CPU durante 20 ataques secuenciales
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7.5 Durante 20 Ataques Secuenciales Desde 2 Hosts Simultáneamente

Se realizaron 20 ataques desde 2 hosts simultáneamente, como se observa en la figura 48, uno de los núcleos se activa y se le asigna una carga adicional del 0,6% al rendimiento global del módulo Raspberry, esto dura aproximadamente 1 segundo y regresa a una etapa estable, con un uso global del CPU del 2%.

Ataques secuenciales con 2 Host

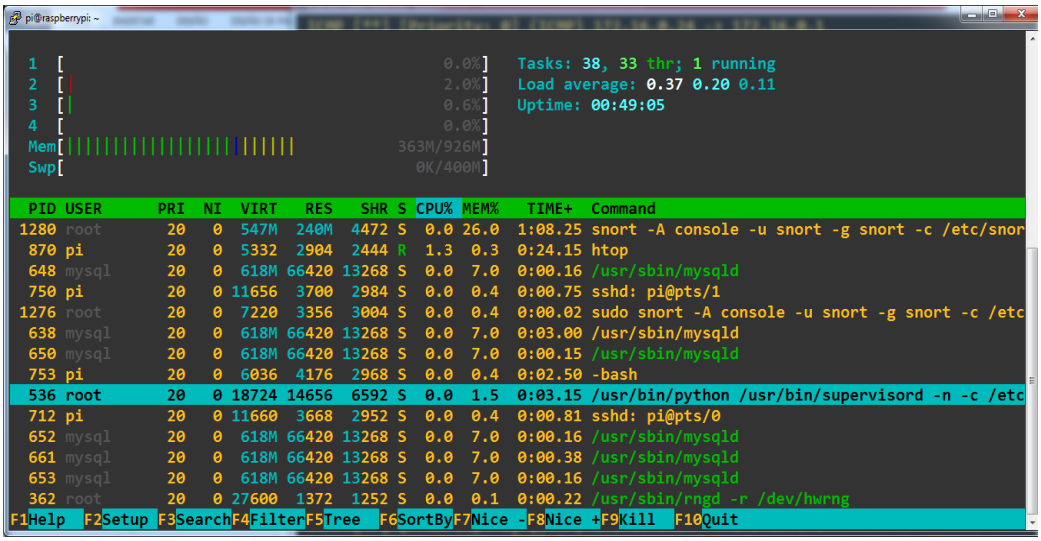

Figura 45. Rendimiento del IDS y del CPU durante 20 ataques secuenciales con 2 host
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7.6 Durante 20 Ataques Secuenciales Desde 3 Hosts Simultáneamente

Se realizó 20 ataques secuenciales como en la anterior prueba, pero en vez desde 3 host simultáneamente. Se puede observar en la figura 49, que se tiene un uso global del CPU del 1,3% de los cuales, 0,7% son netamente del servicio de IDS y el uso de memoria por parte del servicio de IDS se encuentra en el 26%.

Ataques secuenciales con 3 Host

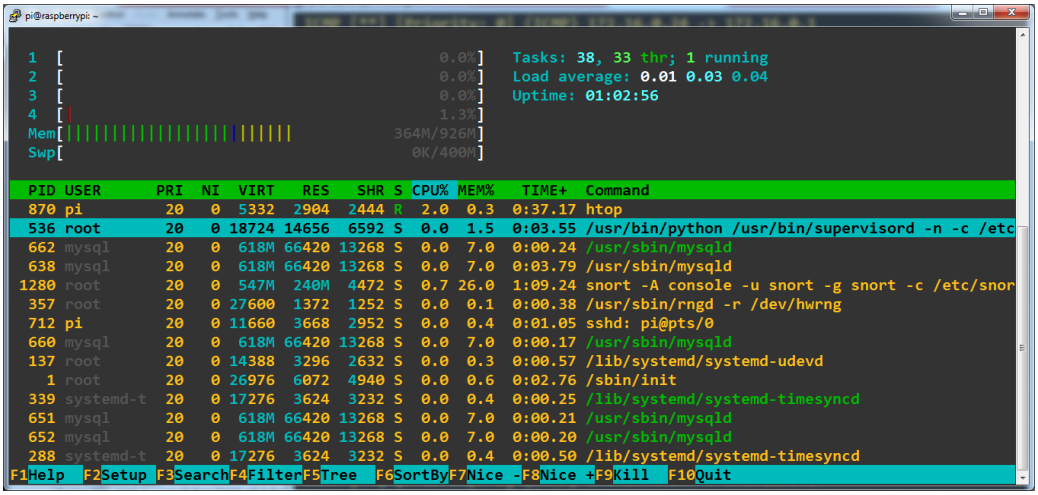

Figura 46. Rendimiento del IDS y del CPU durante 20 ataques secuenciales con 3 host
Elaborado por: Bryan Carate y Francisco Pozo

4.1.7.7 Eficiencia Promedio del uso del CPU

La eficiencia promedio del uso del CPU se la calcula mediante, la sumatoria del uso del CPU de cada prueba realizada, dividido para el número de pruebas, que en este caso es, tres. Esto se puede apreciar en la Tabla 19.

Tabla 19. Eficiencia promedio del uso del CPU

	USO DE CPU				
PRUEBA	**NUCLEO 1**	**NUCLEO 2**	**NUCLEO 3**	**NUCLEO 4**	**TOTAL**
20 ataques con 1 host	0.7 %	1.3 %	0%	0%	2.0 %
20 ataques con 2 hosts	0%	2.0 %	0.6 %	0%	2.6 %
20 ataques con 3 hosts	0%	0%	0%	1.3%	1.3 %
				PROMEDIO	1.96 %

Elaborado por: Bryan Carate y Francisco Pozo

CONCLUSIONES

- La red que se diseñó en GNS3 se utilizó para simular los requerimientos de un escenario PYME en el Ecuador, de tal forma que, se pueda evaluar el módulo Raspberry Pi 3 B con el sistema de detección de intrusos basado en la red, Snort NIDS.
- Dos de los ataques recurrentes a nivel global son: ataques de denegación de servicios y probing. Estas dos fueron las pruebas de ataques internos realizados, el IDS frente a estas evaluaciones de efectividad, indica una taza de paquetes analizados del 96,87% y un promedio de 3,13% de paquetes no resueltos, de este modo se demuestra que, el uso de un módulo Raspberry Pi 3 B como NIDS es una opción válida para un ambiente PYME.
- Snort al ser un proyecto Open Source de Cisco evita costo de licenciamiento, de esta manera descartando problemas legales por uso no autorizado de este software, esto no ocurre frente a otras soluciones IDS como el caso de IBM Qradar, el cual el costo licenciamiento varía por el procesamiento de alertas por segundo y tráfico analizado por minuto o Symantec Critical Systems Protection, donde, su costo de licenciamiento varía por número de nodos; además, se requiere de hardware adicional, ya sea propietario o con requerimientos mínimos, los cuales elevan el costo de la solución de un IDS, en el caso de Snort, se implementó en un módulo Raspberry Pi 3, el cual tiene un costo aproximado de $120, de esta forma se demuestra que el proyecto es de bajo presupuesto y al alcance de una PYME.
- La eficiencia promedio del CPU del módulo Raspberry Pi al momento de realizar los ataques es del 1.96% del uso global del CPU desde que inicializan los ataques, al inicializar el servicio de IDS se aprecia que se le exige al CPU el 100%

aproximadamente durante 9,06 segundos, después de este proceso se estabilizó el sistema y se iniciaron los ataques, el rendimiento del CPU oscila desde 0,7% hasta 2,6 %, evidenciando que al momento de ocurrir incidencias, el IDS tiene suficientes recursos para para brindar un servicio de seguridad al resto de usuarios conectados en un ambiente PYME.

- Basándose en el código orgánico integral penal del Ecuador, el sistema de detección de intrusos que se planteó no viola de ninguna forma los artículos 190 y 232, donde se menciona el uso o modificación no autorizado del sistema IDS o el módulo Raspberry Pi, esto es relevante ya que por cuestiones de pruebas se personalizaron las reglas del IDS, a la vez que se adaptó una protección de acrílico y un ventilador como refrigeración para el módulo Raspberry Pi.
- Dentro de la topología de red PYME que se simuló en GNS3, el módulo Raspberry Pi se conectó a un puerto en el Switch donde se configuró Port Mirroring con el objetivo de permitir la monitorización de los paquetes en la red; al habilitar esta opción en el Switch, este envía copias de trafico al IDS, esto indica que, el IDS no puede cumplir funciones de Firewall porque está trabajando con copias del tráfico que fluye en la red y no está trabajando con el trafico real. Para realizar una función (IDS/Firewall), se debe implementar un firewall dentro del IDS, pero en el momento que un IDS realice tareas adicionales como bloquear conexiones este pasa a realizar funciones de un Sistema de Prevención de Intrusos (IPS), el cual al momento de detectar una intrusión puede tomar una acción como bloquear la conexión que se intenta vulnerar, y un IPS no es parte del objetivo general de esta tesis.

RECOMENDACIONES

- Se puede realizar la implementación de un módulo GPRS adaptado al módulo Raspberry, para así desarrollar una forma en la cual, un administrador de red pueda recibir notificaciones de las alertas a través de un mensaje de texto hacia un número celular.
- Usar el datasheet de DARPA actualizado para evaluar la solución NIDS en una futura versión de Raspberry Pi con mejor rendimiento, en una red de datos física real.
- Implementar una interfaz GUI, para interpretar los datos emitidos por Snort, ya que, al momento, la compatibilidad de la base de datos MySql presenta errores al ser fusionada con MariaDB y presenta bugs.
- Analizar la viabilidad de implementar un IPS en un módulo Raspberry Pi.
- Ya que el Raspberry Pi requiere de alrededor de 5W de potencia, se le puede asignar un UPS dedicado de bajas capacidades en el caso de fallas eléctricas.

LISTA DE REFERENCIAS

2012, I. (06 de NOVIEMBRE de 2012). *UNIVERSIDAD PRIVADA DEL NORTE*. Obtenido de https://vmwareupn.wordpress.com/2012/11/06/que-es-vmware/

Alnour Ibrahim, E. A., Albdri Mohmed, H. S., Abdallah Abusham, J. O., & Mohmed Ali , M. E. (OCTUBRE de 2017). *Sudan University of Science and Technology.* Sudan: Sudan University of Science and Technology. Obtenido de EVALUATION PERFORMANCE OF SNORT: http://repository.sustech.edu//handle/123456789/19375

Aramburu, C. M. (2012). *Bases de datos avanzadas.* Valencia: Universitat Jaume I. Servei de Comunicació i Publicacions.

Arch Linux ARM. (21 de 06 de 2019). *Arch Linux ARM*. Obtenido de https://archlinuxarm.org/

basics, x. (21 de JULIO de 2018). *https://www.xataka.com/basics/que-arduino-como-funciona-que-puedes-hacer-uno.*

BricoGekk. (20 de ABRIL de 2016). *BricoGeek*. Obtenido de https://tienda.bricogeek.com/descatalogado/718-raspberry-pi-2-model-b-1gb.html

CISCO. (s.f.). *https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf.*

Delgado, D. O. (21 de MARZO de 2017). *OpenWebinars*. Obtenido de https://openwebinars.net/blog/que-es-snort/

Destino Negocio. (04 de 11 de 2016). *Destino Negocio*. Obtenido de ¿Cuáles son las amenazas más frecuentes a las que se enfrentan las Pymes?: https://destinonegocio.com/mx/mercado-mx/amenazas-frecuentes-que-enfrentan-pymes/

Echeverri, J., Aristizábal, M., & González, L. (2013). *Reflexiones sobre ingeniería de requisitos y pruebas de software.* Medellín, CO, Colombia: Corporación Universitaria Remington .

EcuRed. (noviembre de 2018). *EcuRed*. Obtenido de mediawiki: https://www.ecured.cu/Snort

EDUCBA (Corporate Bridge Consultancy Pvt Ltd). (26 de 08 de 2018). *EDUCBA*. Obtenido de Raspberry Pi 3 vs Raspberry Pi 2 - Know The 8 USeful Comparison: https://www.educba.com/raspberry-pi-3-vs-raspberry-pi-2/

E-Marmolejo, D. R. (13 de junio de 2018). *HETPRO*. Obtenido de https://hetpro-store.com/TUTORIALES/que-es-raspberry/

ERICKOSVALDOVG. (30 de septiembre de 2014). *WORDPRESS*. Obtenido de https://erickosvaldovg.wordpress.com/2014/09/30/que-es-packet-tracer/

Federal Bureau of Investigation. (17 de 10 de 2017). *Public Service Announcement*. Obtenido de Internet Crime Complaint Center (IC3) | Booter and Stresser Services Increase the Scale and Frequency of Distributed Denial of Service Attacks: https://www.ic3.gov/media/2017/171017-2.aspx

FM, Yúmbal. (21 de 07 de 2018). *Xataka.* Obtenido de Qué es Arduino, cómo funciona y qué puedes hacer con uno: https://www.xataka.com/basics/que-arduino-como-funciona-que-puedes-hacer-uno

G.SOTO, M. (27 de JUNIO de 2016). *Medium Corporation*. Obtenido de https://medium.com/@marvin.soto/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2

Galiano, J. M. (2016). *Implantar scrum con éxito.* Barcelona, España: Editorial UOC.

GENERACIONYOUNG. (28 de AGOSTO de 2018). *MAPFRE*. Obtenido de https://www.generacionyoung.com/tecnologia/mas-tecnologia/para-que-sirve-raspberry-pi-3/

Gómez Vieites, Á. (2014). *Sistemas seguros de acceso y transmisión de datos.* Madrid: RA-MA Editorial.

GOMEZ, G. (2003). *http://www.derecho-internet.org/docs/ids.pdf*.

Gómez, J. L. (2009). *Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas.* Almería: Universidad Almería. Obtenido de http://www.adminso.es/images/8/88/PFC_carlos.pdf

Gómez, R. J. (2016). *Dirección y gestión de proyectos de tecnologías de la información en la empresa.* Barcela, España: FC Editorial.

HALFACREE, U. E. (2012). *https://books.google.es/books?hl=es&lr=&id=g-XhBQAAQBAJ&oi=fnd&pg=PA123&dq=raspberry+pi&ots=Elmy_zBRWu&sig=01OxKdeS-E9Z9k9X1g7qyt6iVIM#v=onepage&q=raspberry%20pi&f=false.*

Hernández Encinas, L. (2016). *La Criptografía.* Madrid: CSIC Consejo Superior de Investigaciones Científicas.

hispananetwork. (2018). *http://tecnologia.glosario.net/terminos-tecnicos-internet/modo-promiscuo-1143.html*.

IBM. (24 de 10 de 2014). *IBM Knowledge Center*. Obtenido de QRadar Network Insights 1091: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_m5_1901.html

IBM. (17 de Ene. de 2018). *https://www.ibm.com/*. Obtenido de https://www.ibm.com/support/knowledgecenter/es/SSWSR9_11.5.0/com.ibm

.mdmhs.overview.doc/entityconcepts.html: https://www.ibm.com/support/knowledgecenter/es/SSWSR9_11.5.0/com.ibm.mdmhs.overview.doc/entityconcepts.html

INISCO. (06 de NOVIEMBRE de 2012). *UNIVERSIDAD PRIVADA DEL NORTE*. Obtenido de https://vmwareupn.wordpress.com/2012/11/06/que-es-vmware/

Lapiedra, R., & Devece, C. (2011). *Introducción a la gestión de sistemas de información en la empresa* (primera ed.). Castellón, España: Universitat Jaume I. Servei de Comunicació i Publicacions.

leonard, j. n. (2000). Examining VMWare. *Dr. Dobbs*, 1.

LIBRE, H. (2014). *https://www.hwlibre.com/que-es-una-placa-sbc/*.

LinuxParty. (06 de JULIO de 2010). *EL Sistema de Deteccion de Intrusos:Snort*. Obtenido de https://www.linux-party.com/57-seguridad/6000-el-sistema-de-deteccion-de-intrusos-snort--windows-y-linux-

Lyon, G. (21 de 06 de 2016). *Nmap: the Network Mapper - Free Security Scanner*. Obtenido de Introduction: https://nmap.org/

Maqueira, J., & Bruque, J. (2012). *Las tecnologías GRID de la información como nueva herramienta empresarial.* Oviedo, ES: Septem Ediciones.

Miarec. (mayo de 2018). *Miarec*. Obtenido de https://www.miarec.com/faq/what-is-port-mirroring

MiaRec, Inc. (25 de 06 de 2019). *MiaRec*. Obtenido de What is port mirroring?: https://www.miarec.com/faq/what-is-port-mirroring

Ministerio de Justicia, Derechos Humanos y Cultos, Subsecretaría de Desarrollo Normativo. (2014). *Código Orgánico Integral Penal.* Quito: Gráficas Ayerve C. A.

Molina Mateos, J. M. (2000). *Seguridad de la información. Criptología.* Córdoba, AR, Argentina: El Cid Editor.

Natour, L. (08 de 08 de 2017). *ABC*. Obtenido de El 43% de los ciberataques se concentran en las pymes: https://www.abc.es/tecnologia/informatica/software/abci-43-por-ciento-ciberataques-concentran-pymes-201708081259_noticia.html

NETWORK, P. T. (24 de ENERO de 2018). *PACKET TRACER NETWORK*. Obtenido de https://www.packettracernetwork.com/features/packettracer-vs-gns3.html

Neuman. (2015). https://books.google.es/books?hl=es&lr=&id=9wcvDwAAQBAJ&oi=fnd&pg=PR5&dq=gns3+network+simulation&ots=aDJg9vTWN2&sig=jsG7dyez_l0vyTttlsPY18j4D8o#v=onepage&q=gns3%20network%20simulation&f=false.

Ochando, P. D. (01 de Feb. de 2013). *ccdoc-basesdedatos*. Recuperado el 15 de Ene. de 2018, de ccdoc-basesdedatos: http://ccdoc-basesdedatos.blogspot.com/2013/02/modelo-entidad-relacion-er.html

OPNET Projets Team. Customized OPNET Simulator Projects. (21 de 06 de 2019). *OPNET Network Simulator*. Obtenido de Opnet Projects: http://opnetprojects.com/opnet-network-simulator/

Oppel, A. (2010). *Fundamentos de bases de datos.* México, D.F. MX: McGraw-Hill Interamericana.

Oracle VM VirtualBox. (22 de 06 de 2019). *Oracle VM VirtualBox Manual*. Obtenido de Chapter 1. First Steps: https://www.virtualbox.org/manual/ch01.html

Ortega Triguero, J., & López Guerrero, M. Á. (Castilla). *Introducción a la criptografía: historia y actualidad.* 2006: Ediciones de la Universidad de Castilla-La Mancha.

OVH innovation for Freedom. (24 de 06 de 2019). *¿Qué es un ataque DDoS? - OVH*. Obtenido de ¿Qué es un ataque DDoS?: https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml

Pickett, P. (13 de 05 de 2019). *The Balance Careers*. Obtenido de How Open-Source Software Works: https://www.thebalancecareers.com/what-is-open-source-software-2071941

PowerData. (18 de Nov. de 2017). *PowerData*. Recuperado el 15 de Ene. de 2018, de PowerData: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/mejora-las-relaciones-con-los-clientes-con-un-master-data-management

Rafael, L., & Carlos, D. (2011). *Introducción a la gestión de sistemas de información en la empresa.* Castellón, España: Universitat Jaume I. Servei de Comunicació i Publicacions.

Red Hat, Inc. (25 de 06 de 2019). *Opensource.com*. Obtenido de What is open source?: https://opensource.com/resources/what-open-source

Rincón, C., & Acuero, A. (2008). Aspectos de diseño de un entorno de programación colaborativo. *Revista Venezolana de Información, tecnología y conocimiento*, 23.

Ruedas, J. G. (2016). *Dirección y gestión de proyectos de tecnologías de la información en la empresa.* Madrid, España: FC Editorial.

S.A, C. D. (s.f.). *UNOCERO*. Obtenido de https://www.unocero.com/noticias/raspbian-sistema-operativo-gratuito-para-la-raspberry-pi/

Scott, C., Wolfe, P., & Hayes, B. (2004). *Snort for dummies.* Hoboken, NJ: Wiley Pub.

Singh, S., & Singh, J. (2015). SSMDM: An Approach of Big Data for Semantically Master Data Management. *IEEE*, 1.

sistemas, C. (27 de MARZO de 2013). *Confirma sistemas*. Obtenido de https://www.confirmasistemas.es/es/contenidos/canal-basics/que-es-el-spoofing

Sysmantec Corporation. (24 de 06 de 2019). *Symantec Enterprise.* Obtenido de Symantec Critical System Protection: https://www.symantec.com/content/en/us/partners/media/smb_resources/scsp-fs-en.pdf

Tapia Cuesta, J. A. (2017). *PROPUESTA DEL DISEÑO DE UN MANUAL DE PRESUPUESTO PARA LA MICROEMPRESA EQUIPOS COLOMA EN LA CIUDAD DE QUITO PARA EL PERIODO 2015-2016.* Quito: Quito: UCE. Obtenido de http://www.dspace.uce.edu.ec/handle/25000/15987

TELECTRONICA. (29 de ABRIL de 2018). *TELECTRONICA*. Obtenido de https://telectronika.com/articulos/que-es-gns3/

Telectrónika. (29 de 04 de 2018). *GNS3 Guía Introductoria: Características y Requerimientos Mínimos*. Recuperado el 2019, de GNS3 Guía Introductoria: Características y Requerimientos Mínimos: https://telectronika.com/articulos/que-es-gns3/

Thompson, M. (21 de 06 de 2012). *FrontPage - Raspbian*. Obtenido de Welcome to Raspbian: https://www.raspbian.org/

TRENDnet, inc. (2019). *TRENDnet*. Obtenido de https://www.trendnet.com/langsp/products/product-detail?prod=150_TU2-ET100

TRENDnet, inc. (2019). *TRENDnet*. Obtenido de https://www.trendnet.com/langsp/products/product-detail?prod=150_TU2-ET100

Universidad Complutense Madrid. (2019). *UCM-Proyecto de Innovación Software libre para ciencias e ingenierías*. Obtenido de GNS3: https://www.ucm.es/pimcd2014-free-software/gns3

Valencia., M. J. (17 de 05 de 2019). *Derecho Ecuador*. Obtenido de MICROEMPRESA: https://www.derechoecuador.com/microempresa

Valonso. (6 de SEPTIEMBRE de 2018). *El blog del informtico*. Obtenido de http://blog-del-linformatico.blogspot.com/2008/09/simulador-opnet.html

Vega Villacís, G. (14 de MARZO de 2017). *3CIENCIAS*. Obtenido de VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA UNIVERSIDAD TECNICA DE BABAHOYO: https://www.3ciencias.com/wp-content/uploads/2017/03/ART5.pdf

Virtualization, O. (18 de JULIO de 2015). *ORACLE*. Obtenido de https://blogs.oracle.com/virtualization/oracle-vm-virtualbox-extension-pack-v2

VMware, Inc. (21 de 06 de 2019). *Workstation Pro - VMware Products : Windows Virtualization for Everyone*. Obtenido de Workstation Pro - VMware Products: https://www.vmware.com/co/products/workstation-pro.html

Wagner, B. (13 de Julio de 2017). *Hackernoon*. Obtenido de Hackernoon: https://hackernoon.com/xml-vs-json-shootout-which-should-i-use-in-sql-server-7eefa4dc7553

Wang, L., Ming, X., & You, J. (2009). The Steps and Methodology of Identifying Master Data from Business Processes. *2009 WRI World Congress on Software Engineering* (pág. 5). IEEE.

Wikipedia. (16 de NOVIEMBRE de 2018). *https://es.wikipedia.org/wiki/Raspberry_Pi#Raspberry_Pi_3_Model_B+%5B53%5D%E2%80%8B.*

WIKIPEDIA. (6 de MAYO de 2019). *WIKIPEDIA*. Obtenido de https://es.wikipedia.org/wiki/VMware

俺の技術メモ. (30 de marzo de 2016). *Raspberry Pi 2 Model B とRaspberry Pi 3 Model B の比較*. Obtenido de http://xn--u9j0md1592aqmt715c.net/raspberrypi-2-3-diff/